資安職能訓練
電子郵件安全
換證課程

行政院國家資通安全會報技術服務中心 編製

課程簡介

- 課程著重在「防護」及「管理」，以期落實電子郵件安全控管，強化資訊人員對於電子郵件安全的技術與管理能力，提升組織進行電子郵件威脅之安全防護能力，維護電子郵件服務安全與正常運作
- 適用對象：已取得本門課程證書之學員

課程學習目標

- 本課程目標旨在強化資訊人員對於電子郵件安全的技術與管理能力
- 提升組織進行電子郵件威脅之安全防護能力
- 維護電子郵件服務安全與正常運作

電子郵件安全換證課程 3

課程學習目標

- **知識(Knowledge)方面的學習目標：**
  - K1瞭解電子郵件系統面臨的弱點、威脅及防護
  - K2瞭解電子郵件運作與設定
  - K3瞭解電子郵件相關安全防護機制
  - K4瞭解電子郵件各種分析技術與機制
  - K5瞭解電子郵件安全管理
  - K6瞭解電子郵件服務的新發展

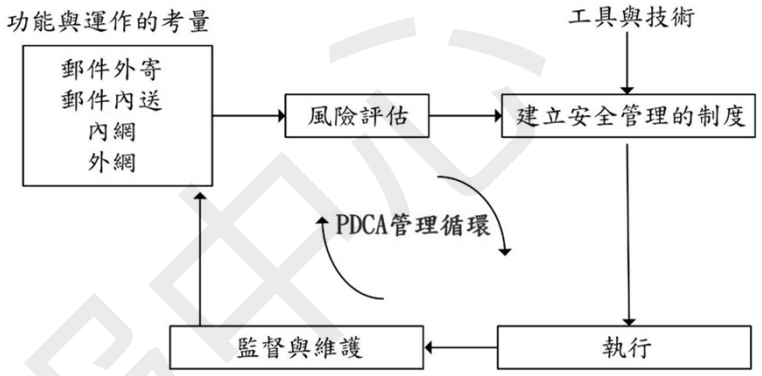
第1單元
電子郵件的弱點與威脅

單元學習目標

- 瞭解電子郵件系統在伺服器、使用者及協定本身之弱點
- 瞭解電子郵件系統在機密性、完整性及可用性的威脅，並針對電子郵件系統之弱點與威脅提供防護建議

建立電子郵件使用的風險意識

- 電子郵件因行動裝置與雲端服務帶來的方便性，也提高了風險程度
- 技術無法解決所有的問題，要以**法規面**為基礎建立管理制度，在風險評估之後做適當的導入

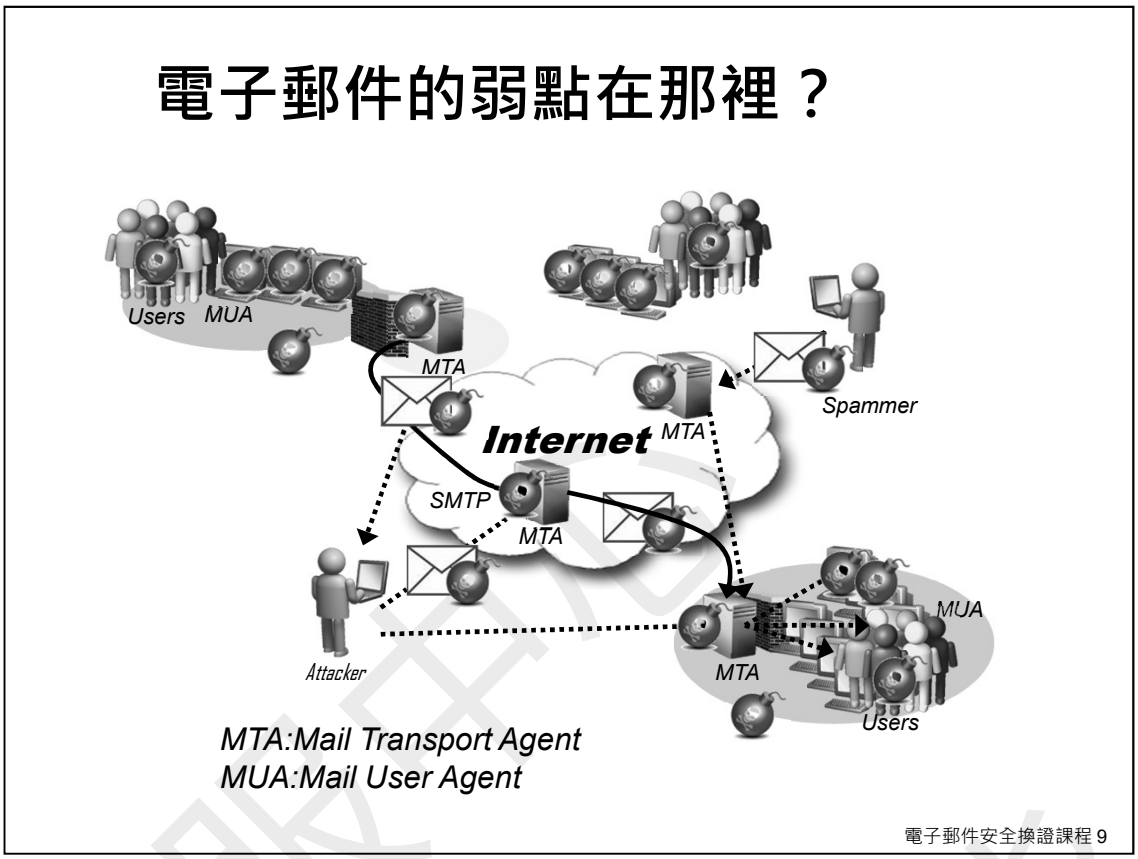


電子郵件安全換證課程 7

- 大多數的機構都已經建置了電子郵件系統，但是未必有一套完善的安全管理制度。
- 即使投注資金建置各種軟硬體設施，未必真正能達到防護、合規與保護的效果。
- 使用者要有電子郵件使用安全的風險意識。
- 電子郵件使用的安全管理應該遵循PDCA的管理循環，才能因應變化中的環境威脅。
- 電子郵件系統的建置應搭配風險評估，在適當的成本下建置合用的架構。

建立電子郵件系統安全管理程序

- 政府機關宜參閱「**資訊系統風險評鑑參考指引**」與「**資通安全責任等級分級辦法**」，對電子郵件系統的安全等級進行評定，再以評定的安全等級確認各項適用建議
- 針對電子郵件安全的弱點、威脅及風險程度，從管理面與技術面參考「**安全控制措施參考指引**」，以「規劃(Plan)」、「執行(Do)」、「檢查(Check)」及「行動(Act)」管理循環構面，在國際資安管理經典(如CNS/ISO/IEC 27001與NIST SP800-53rev4) 的基礎上確認安全控制措施



- MTA：Mail Transfer Agent，即郵件傳輸代理。電子郵件的傳輸主要依靠MTA來完成，它負責郵件儲存和轉發。MTA根據電子郵件的地址找出相應的郵件伺服器，將信件在伺服器之間傳輸並將收到的郵件進行緩衝或者選擇送往下一個MTA主機。MTA是用在郵件服務端的軟體，它接收外部主機寄來的信件併發送給目的MTA。
- MUA：Mail User Agent，即郵件用戶代理。不論是送信還是收信，客戶端都需要通過各個操作系統提供的MUA才能夠使用郵件系統。比如Windows的Outlook Express。MUA主要的功能就是接收郵件主機的電子郵件，並提供用戶瀏覽與編寫郵件的功能。MUA是用於客戶端的軟體，同時也是用戶和MTA之間的介面。
- 電子郵件的弱點在那裏？
  - ✓ 在電子郵件伺服器中(MTA)
    - ➢ Mail server本身就可能會具有弱點，不論Mail server放在DMZ或是放在機關內部網路，由於Mail Server要負責收外面網際網路進來的信件，所以防火牆必須開放外部任何IP都可以連線Mail server的25 port，一但Mail server有弱點存在被駭客運用時，就可能造成機關的資訊風險與損害。
  - ✓ 在電子郵件用戶端(MUA)
    - ➢ MUA端的程式也可能會有弱點，像使用者常用的Outlook或者Thunderbird，駭客可能編寫特殊的信件寄給使用者，這些特殊信件裡面可能包含了惡意的圖檔，只要使用者一開啟這惡意變造的信件，揭露了Outlook的弱點，就可能在使用者的電腦上植入後門程式。
  - ✓ SMTP協定本身的設計
    - ➢ SMTP協定本身就是電子郵件系統中很大的弱點，各位已經稍微了

解SMTP協定，等一下我們再談SMTP協定有甚麼樣的弱點。

- ✓ 電子郵件系統的部署方式
  - ➢ 電子郵件系統的錯誤部署也可能造成弱點，例如：電子郵伺服器未置於DMZ區、電子郵件防禦機制可能被跳過、或者允許內部人員直接存取外部的郵件伺服務等。
- ✓ 電子郵件使用人員
  - ➢ 在電子郵件系統安全裡面，目前最難克服的還是電子郵件使用人員的問題，駭客透過電子郵件社交工程的攻擊手法，誘使使用者開啟信件、點選信件中的惡意連結、或者開啟惡意的附件檔案，而導致後門程式被植入。所以有關電子郵件社交工程一些問題，基本上不是技術性問題，而是人性的問題。

電子郵件部署的弱點

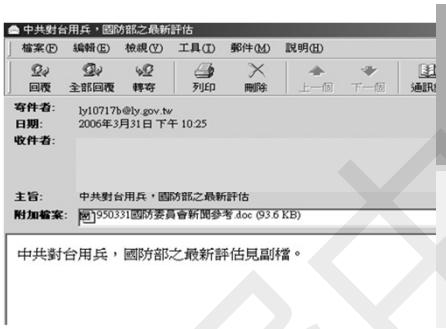
- 電子郵件伺服器未置於DMZ區
  - –公開服務伺服器未與內網區隔
- 防護機制(Anti-virus、Anti-spam)可以被規避
  - –為了可用性考量造成的防護疏失
- 開放下載外部私人信件(POP3/IMAP4/Webmail)
  - –變成防護的漏洞
- SMTP(TCP Port 25)內到外的連線是開放的
  - –無法控管的外寄信件
  - –私下發送不當信件的問題

重新規劃部署方式

- 電子郵件部署的弱點
- 是因為電子郵件系統的不當部署方式，而導致的漏洞：
  - ✓ 電子郵件伺服器未置於DMZ區，致使公開服務伺服器未與內網區隔，一旦公開服務伺服器被入侵，就變成進入內網最佳跳板。
  - ✓ 防護機制(AntiVirus、AntiSpam…)可以被規避，通常因為可用性考量造成的防護疏失。
  - ✓ 開放下載外部私人信件(POP3/IMAP4/Webmail)，變成電子郵件防毒、防垃圾與資料外洩的防護漏洞。
  - ✓ SMTP(TCP 25 port)內到外的連線是開放的，無法控管的使用者外寄信件，導致資料外洩或變成垃圾信件寄件者的跳板。
- 建議應定期檢視電子郵件系統的規劃及部署方式，是否有防護架構上的漏洞。

電子郵件使用人員的弱點

- 興趣/嗜好：對特定領域的資訊有高度興趣
- 貪心：撿便宜的個性
- 好奇：探索八卦訊息的個性
- 不在意：沒那麼倒楣、沒那麼嚴重的想法
- 偽造業務相關的攻擊信件：



這是最大的風險
也是最難控管的環節

加強人員安全認知訓練

電子郵件安全換證課程 11

- 電子郵件使用人員的弱點
- 由於下列人性的弱點，讓駭客可以透過社交工程攻擊手法來入侵內部的電腦：
  - ✓ 興趣/嗜好：對特定領域的資訊有高度興趣。
  - ✓ 貪心：撿便宜的個性。
  - ✓ 好奇：探索八卦訊息的個性。
  - ✓ 不在意：沒那麼倒楣、沒那麼嚴重的想法。
- 攻擊者運用電子郵件社交工程的手法，寄送大量垃圾或廣告郵件，來引誘/詐騙電子郵件使用者，點選連結或執行程式，導致病毒或後門的植入。在電子郵件安全防護上，這個弱點造成最大的風險，但也是最難控管的環節。
- 只有透過持續不斷「加強人員安全認知訓練」來提高電子郵件使用人員的安全警覺性，也可以藉由電子郵件社交工程的演練來了解機關在人員安全認知的程度，針對沒有警覺性的使用者，施予強化訓練。

破壞「機密性」的威脅(1/2)

- **駭客竊取機密資料**
  - –攔截未加密的電子郵件傳送(SMTP弱點)
    - ➢ 風險：郵件中機密資訊外洩
    - ➢ 風險：內部IP位址及傳送路徑外洩
  - –攔截未加密的用戶帳號及密碼(如：POP3、Webmail/HTTP)
    - ➢ 風險：用戶來往郵件中的機密資訊外洩與偽冒該用戶
  - –直接攻擊電子郵件伺服器植入後門(MTA弱點)
    - ➢ 風險：電子郵件伺服器所有進出郵件外洩
    - ➢ 風險：所有電子郵件帳號外洩

電子郵件安全換證課程 12

- 破壞「機密性」的威脅
- 駭客竊取機密資料的威脅、其相對運用的弱點及產生的風險如下：
  - ✓ 攔截未加密的電子郵件傳送(SMTP弱點)：
    風險：郵件中機密資訊外洩。
    風險：內部IP位址及傳送路徑外洩。
  - ✓ 攔截未加密的用戶帳號及密碼(如：POP3、Webmail/HTTP)：
    風險：用戶來往郵件中的機密資訊外洩與偽冒該用戶。
  - ✓ 直接攻擊電子郵件伺服器植入後門(MTA弱點)：
    風險：電子郵件伺服器所有進出郵件外洩。
    風險：所有電子郵件帳號外洩。

破壞「機密性」的威脅(2/2)

- **駭客竊取機密資料**
  - –透過電子郵件植入後門程式到電子郵件用戶端電腦(MUA、人性弱點)
    - 風險：用戶端電腦檔案外洩
    - 風險：用戶端個人資料及密碼外洩
    - 風險：用戶存取行為及連線內容被監聽
    - 風險：監聽內部帳號/密碼，向內部網路擴大攻擊

目前最主要的威脅

- 破壞「機密性」的威脅
- 駭客竊取機密資料的威脅、其相對運用的弱點及產生的風險如下：
  - ✓ 透過電子郵件植入後門程式到電子郵件用戶端電腦(MUA、人性弱點)，這也是目前電子郵件安全中最主要的威脅：
    - 風險：用戶端電腦檔案外洩。
    - 風險：用戶端個人資料及密碼外洩。
    - 風險：用戶存取行為及連線內谷被監聽。
    - 風險：監聽內部帳號/密碼，向內部網路擴大攻擊。

破壞「完整性」的威脅

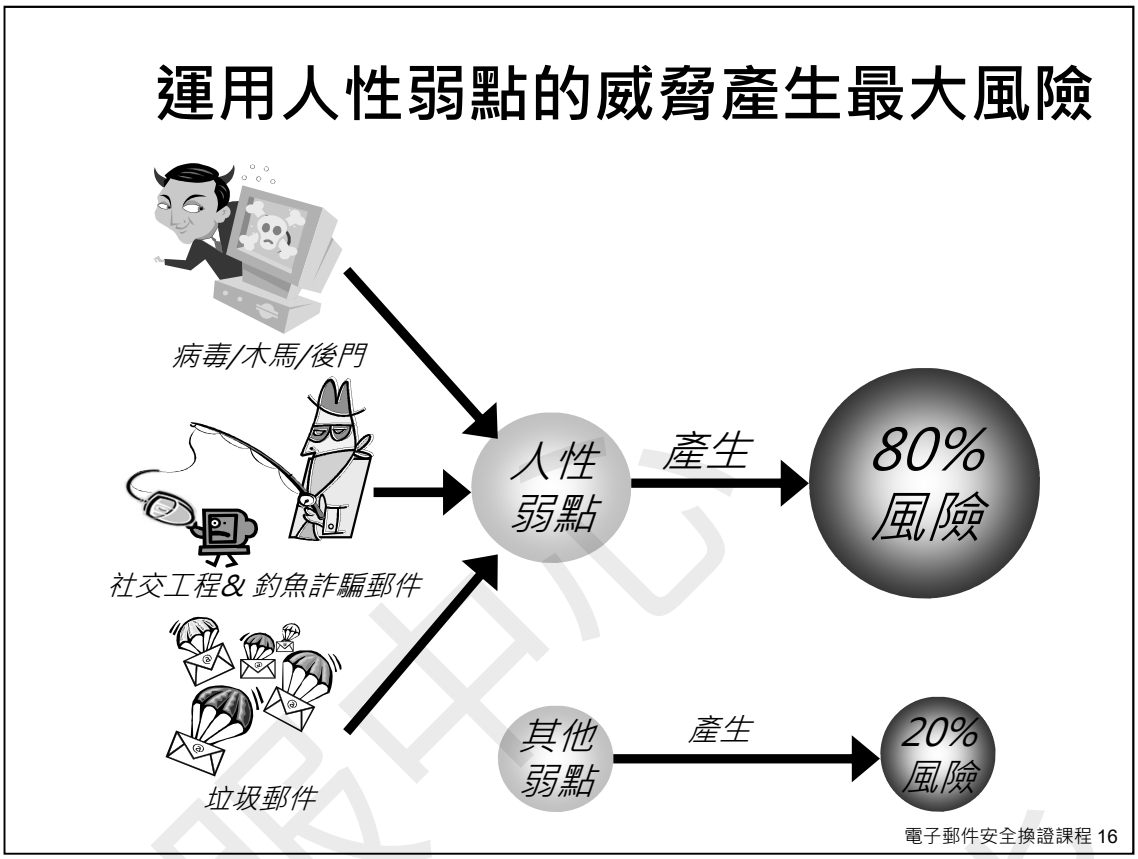
- 駭客偽冒身分
  - –以主管身分寄送後門程式引誘使用者開啟(SMTP、人性弱點)
    - 風險：使用者電腦系統被植入後門導致資訊外洩
  - –以他人身分發送毀謗不實言論(SMTP弱點)
    - 風險：被偽冒人遭訴訟
- 駭客竄改正常信件內容
  - –植入病毒、蠕蟲及後門(SMTP弱點)
    - 風險：用戶端電腦資訊外洩
  - –變造信件內容(SMTP弱點)
    - 風險：收到錯誤資訊導入計算錯誤、決策判斷錯誤

- 破壞「完整性」的威脅
  - ✓ 駭客偽冒身分的威脅：
    - ➢ 以主管身分寄送後門程式引誘使用者開啟(SMTP、人性弱點)。
      風險：使用者電腦系統被植入後門導致資訊外洩。
    - ➢ 以他人身分發送毀謗不實言論(SMTP弱點)。
      風險：被偽冒人遭訴訟。
  - ✓ 駭客竄改正常信件內容的威脅：
    - ➢ 植入病毒、蠕蟲及後門(SMTP弱點)。
      風險：用戶端電腦資訊外洩。
    - ➢ 變造信件內容(SMTP弱點)。
      風險：收到錯誤資訊導入計算錯誤、決策判斷錯誤。

破壞「可用性」的威脅

- 駭客癱瘓郵件伺服器
  - 以**電子郵件炸彈**攻擊郵件伺服器(SMTP弱點)
    - 風險：郵件系統無法使用導致業務無法執行
- 廣告/詐騙/釣魚信件
  - 佔用頻寬及信箱空間(SMTP弱點、人性弱點)
    - 風險：郵件系統資源被佔用導致業務無法順利完成
  - 大量與工作無關的信件 (SMTP弱點、人性弱點)
    - 風險：正常工作被干擾導致生產力降低
  - 誘騙收件人財務或個資(SMTP弱點、人性弱點)
    - 風險：收件人財務的損失與導致訴訟
  - 業務相關之標的式攻擊信件
    - 風險：導致機密資訊外洩

- 破壞「可用性」的威脅
  - ✓ 駭客癱瘓郵件伺服器的威脅：
    - ➢ 以電子郵件炸彈攻擊郵件伺服器(SMTP弱點)。
      風險：郵件系統無法使用導致業務無法執行。
  - ✓ 廣告/詐騙/釣魚信件：
    - ➢ 佔用頻寬及信箱空間(SMTP弱點、人性弱點)。
      風險：郵件系統資源被佔用導致業務無法順利完成。
    - ➢ 大量與工作無關的信件 (SMTP弱點、人性弱點)。
      風險：正常工作被干擾導致生產力降低。
    - ➢ 誘騙收件人財務或個資(SMTP弱點、人性弱點)。
      風險：收件人財務的損失及導致訴訟。
    - ➢ 業務相關之標的式攻擊信件。
      風險：導致機密資訊外洩。



- 運用人性弱點的威脅產生最大的風險
- 以社交工程手法寄送「病毒/木馬/後門」、「社交工程、釣魚詐騙郵件」及「垃圾郵件」，來揭露「人性弱點」，所造成的風險佔電子郵件安全風險的80%，其他弱點所造成的風險只有20%。機關應積極思考如何降低因人性弱點所導致的風險。

社交工程攻防演練

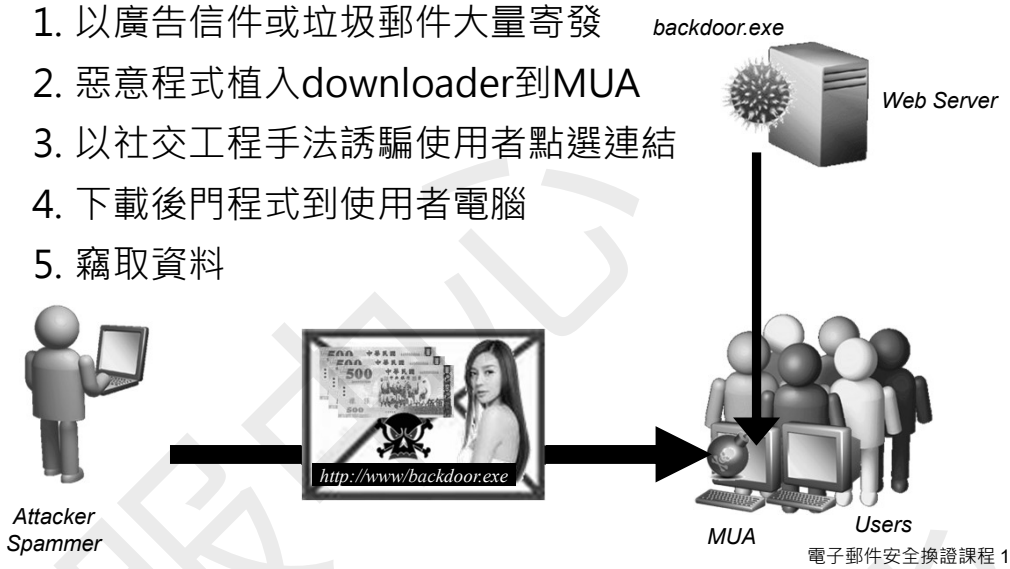
- 假造寄信人以及內容，引誘收信人開啟郵件、開啟附件，或是點按超連結
- 經由後台蒐集統計的結果來瞭解受測者的警覺程度高低
- 可洽詢使用「行政院國家資通安全會報技術服務中心」的社交工程攻防演練平台

資料來源：Phish Insight，趨勢科技網站，106年10月

- 可運用免費的服務進行社交工程攻防演練。
- 學員可以參考使用趨勢科技的Phish Insight，或是搜尋網路上主要資安廠商所提供的工具來練習。

混合模式的威脅(1/2)

- **目前駭客及攻擊發送者多已採用混合模式的攻擊手法**
  1. 以廣告信件或垃圾郵件大量寄發
  2. 惡意程式植入downloader到MUA
  3. 以社交工程手法誘騙使用者點選連結
  4. 下載後門程式到使用者電腦
  5. 竊取資料



電子郵件安全換證課程 18

- 混合模式的威脅(1/2)
- 目前駭客及攻擊發送者多已採用**混合模式**的攻擊手法，在一封郵件中包含了下列威脅：

  ✓ 以廣告信件或垃圾郵件大量寄發。
  ✓ 惡意程式植入downloader到MUA。
  ✓ 以社交工程手法誘騙使用者點選連結。
  ✓ 下載後門程式到使用者電腦。
  ✓ 竊取資料

混合模式的威脅(2/2)

- **一旦電子郵件用戶端電腦被植入後門程式後，駭客可以進行下列的惡意行為：**
  - 竊取硬碟中的文件檔案資料
  - 監聽鍵盤輸入的敏感資料(密碼/帳號)
  - 遠端遙控用戶端電腦
  - 攻擊其他內部的電腦
  - 攻擊別人的跳板

電子郵件安全換證課程 19

- 混合模式的威脅(2/2)
- 一旦電子郵件用戶端電腦被植入後門程式後，駭客可以**進行下列的惡意行為**：
  - ✓ 竊取硬碟中的文件檔案資料。
  - ✓ 監聽鍵盤輸入的敏感資料(密碼/帳號)。
  - ✓ 遠端遙控用戶端電腦。
  - ✓ 攻擊其他內部的電腦。
  - ✓ 攻擊別人的跳板。

相關案例：遠東銀行SWIFT遭駭事件

- 遠東銀行SWIFT遭駭事件是臺灣首例，創下臺灣銀行遭駭盜轉金額新紀錄
- 全球金融機構通用的**SWIFT通訊系統**是銀行間交易中交換結構化的電子訊息的平臺，處理支付和交易結算等商業流程
- 駭客利用SWIFT系統的漏洞，或網路進行攻擊，來取得SWIFT系統的操作權限，植入惡意程式，將該銀行的資金轉出
- SWIFT要求會員銀行遵守多項強制**控制措施**，並自2018年起對會員銀行進行稽核

- 攻擊銀行轉帳交易系統SWIFT的系統事件，最早出現在2013年，孟加拉的Sonali Bank遭到駭客攻擊，成功盜領該銀行25萬美元的資金，駭客透過網路在銀行內部電腦植入惡意程式keylogger，竊取相關的系統帳號和密碼，取得操作權限，並使用SWIFT系統傳送偽造的轉帳申請。
- 遠東銀行SWIFT遭駭事件就是一種網路的資安攻擊，發生的原因通常有多種，包括內賊、網路與系統的漏洞、運作的特定環節發生問題。防護的方法包括提高資安的警覺，迅速修補漏洞，遵循並強化被要求執行的安全控制措施，並且在事件發生時透過迅速通報與資安聯防降低損失。
- **社交工程與電子郵件的混合式攻擊往往是後續破壞行動開始的序幕**，必須封阻這些管道。

網頁郵件(Webmail)的威脅

- 透過Web 瀏覽器以連結存取網頁伺服器，來收發讀寫電子郵件，雖然非常方便，卻潛藏許多使用上的風險：
  - HTTP通訊未經加密信件內容可能會被側錄而外洩
  - 機關未管制使用私人的網頁郵件導致防護的漏洞，使外部個人郵件之病毒威脅入侵內部網路
  - 未加密的Webmail帳號及密碼被監聽外洩
  - 使用公共場所的電腦來收發網頁郵件，可能會因為該設備被植入鍵盤側錄程式，而造成帳號、密碼等資料的外洩

- 網頁郵件(Webmail)的威脅
- 透過Web 瀏覽器以連結存取網頁伺服器，來收發讀寫電子郵件，雖然非常方便，卻潛藏許多使用上的風險：
  - ✓ HTTP通訊未經加密信件內容可能會被側錄而外洩。
  - ✓ 機關未管制使用私人的網頁郵件導致防護的漏洞，使外部個人郵件之病毒威脅入侵內部網路。
  - ✓ 未加密的Webmail帳號及密碼被監聽外洩。
  - ✓ 使用公共場所的電腦來收發網頁郵件，可能會因為該設備被植入鍵盤側錄程式，而造成帳號、密碼等資料的外洩。

行動通訊設備使用電子郵件之威脅

威脅	防護方法
行動通訊設備遺失	開啟密碼之設定 資料加密機制 雲端資料移除服務
收發電子郵件時之通訊攔截	VPN通訊SSL, TLS加密訊息
智慧型手機之惡意程式碼	手機防毒軟體 避免安裝來源不明的軟體 避免開啟不明來源的信件
雲端資料儲存	加密保護

註：行動通訊位置隱私外洩問題，如：Facebook 打卡、相片含GPS座標資訊等，應提高警覺避免不知不覺中外洩位置資訊

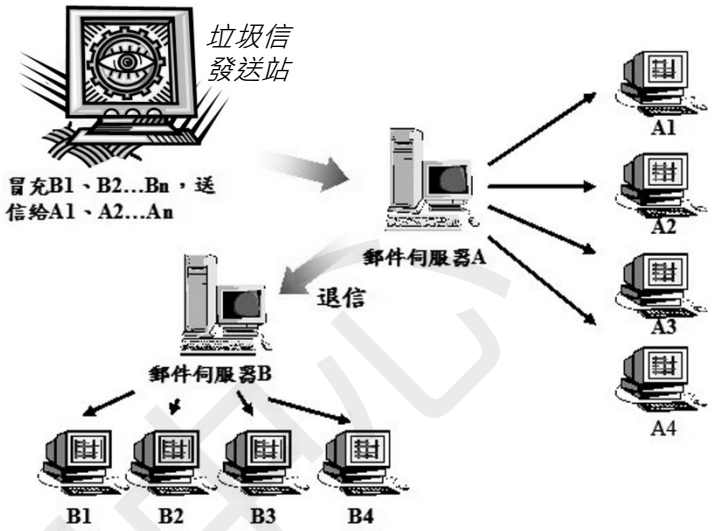
- 行動通訊設備使用電子郵件之威脅
- 由於智慧型手機的普遍使用，現今行動通訊設備存取電子郵件的情形可以說是基本需求，因此相關於行動通訊設備使用電子郵件之威脅及其防護方法，說明如下：
  - ✓ 行動通訊設備遺失的威脅
    其防護建議為：
    開啟行動設備開機之密碼之設定，使用行動設備前需要輸入密碼，若密碼錯誤次數達指定次數以上時可清除行動設備上之資料。
    針對行動設備上之機密資料進行加密加密保護，以避免資料外洩。
    啟用雲端資料移除服務，當行動設備遺失後可透過雲端設定將設備中的資料刪除。
  - ✓ 收發電子郵件時之通訊攔截的威脅
    其防護建議為：
    啟用VPN通訊或者SSL/TLS進行信件傳輸的加密保護。
  - ✓ 智慧型手機之惡意程式碼的威脅
    其防護建議為：
    可考慮採用行動通訊設備上之防毒軟體，但目前此類軟體之效果不大，因此，主要還是避免安裝不明來源的軟體，或開啟不明的信件。
  - ✓ 雲端資料儲存外洩威脅
    其防護建議為：
    將送上雲端備份或儲存之資料或信件，進行加密保護，即使雲端資料被讀取也無法得知其內容。
- 註：行動通訊位置隱私外洩問題，如：Facebook 打卡、相片含GPS座標資訊等，應提高警覺避免不知不覺中外洩位置資訊。

郵件炸彈(Email Bomb)

- 郵件炸彈攻擊行為
  - 是指發送端以同一封郵件於短時間內，**對某收信端進行多次寄送**，以試圖困擾該收信者，甚至阻絕該收信端的郵件傳輸服務
- 郵件炸彈之處理
  - 收到郵件炸彈時，可檢查郵件標頭的訊息(如Received: …)，試著找出郵件真正的來源，並與來源站台的管理者進行通報，以制止這類攻擊
  - 發送者通常會偽冒郵件來源，讓追查郵件來源變得更為困難(因為從郵件標頭的From:得知的訊息，有可能是偽冒的)

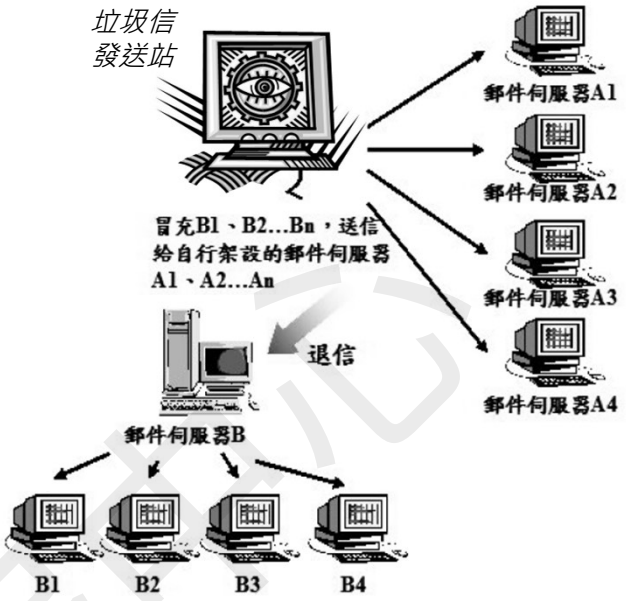
- 郵件炸彈(Email Bomb)
  - ✓ 郵件炸彈攻擊行為
    是指發送端以同一封郵件於短時間內，對某收信端進行多次寄送，以試圖困擾該收信者，甚至阻絕該收信端的郵件傳輸服務。
  - ✓ 郵件炸彈之處理
    收到郵件炸彈時，可檢查郵件標頭的訊息(如Received: ...)，試著找出這封郵件真正的來源，並與來源站台的管理者進行通報，以制止這類攻擊。
    發送者通常會偽冒郵件來源，讓追查郵件來源變得更為困難(因為從郵件標頭的From:得知的訊息，有可能是偽冒的)。

退信攻擊模式(1)- 基本型



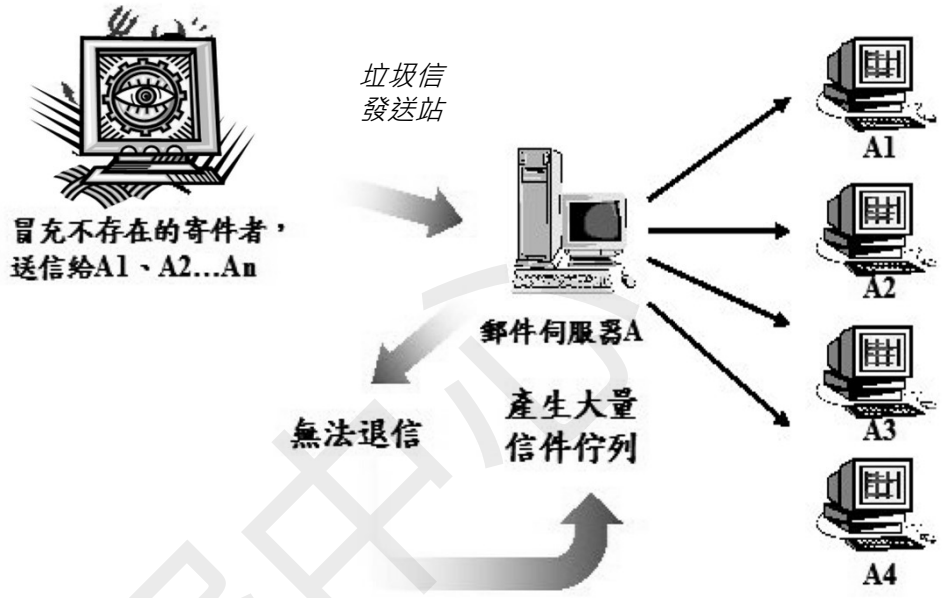
- 退信攻擊模式(1)- 基本型
  1. 攻擊者冒充B1,B2....Bn寄信給A1, A2...An(其實A1, A2...An是不存在的) 。
  2. 導致郵件伺服器A大量退信給郵件伺服器B。
  3. 受害者為郵件伺服器A與B。

退信攻擊模式(2)-變化模式(一)



- 退信攻擊模式(2)- 變化模式(一)
  1. 攻擊者冒充B1,B2....Bn，送信給自行架構的郵件伺服器A1, A2...An。
  2. 導致郵件伺服器A1, A2...An 大量退信給郵件伺服器B。
  3. 受害者為郵件伺服器 B。

退信攻擊模式(3)-變化模式(二)



電子郵件安全換證課程 26

- 退信攻擊模式(3)-變化模式(二)
  1. 攻擊者冒充不存在的寄件者，寄信給A1, A2...An。
  2. 導致郵件伺服器A無法退信，產生大量的信件佇列。
  3. 受害者為郵件伺服器 A。

電子郵件系統密碼猜測攻擊

- 密碼猜測的管道
  - POP3/IMAP4之登入密碼
  - SMTP AUTH之發信密碼
- 密碼猜測攻擊的目的
  - 取得發送垃圾信件的管道
  - 竊取信箱中的信件內容
  - 入侵其他系統(被猜中的密碼可能「也是」其他系統的密碼)
- 密碼猜測的防護
  - 密碼強度要求(長度、複雜度、更換頻率)
  - 登入失敗之警告與異常統計
  - 自動延遲或封鎖密碼猜測之攻擊來源

- 電子郵件系統密碼猜測攻擊，也是目前最常見的攻擊手法之一：
  - ✓ 密碼猜測的主要管道：
    POP3/IMAP4之登入密碼及SMTP AUTH之發信密碼(發信時認證)。
  - ✓ 其密碼猜測攻擊的目的為：
    取得發送垃圾信件的管道、竊取信箱中的信件內容及入侵其他系統(被猜中的密碼可能「也是」其他系統的密碼)。
  - ✓ 針對電子郵系統密碼猜測的防護建議為：
    密碼強度要求(長度、複雜度、更換頻率)、登入失敗之警告與異常統計、及自動延遲或封鎖密碼猜測之攻擊來源。

當密碼被猜中後

- **問題狀況**
  - 大量信件寄出
  - 收到大量退信
  - Mail Queue中有大量待寄信件
  - 被列為寄件黑名單
- **緊急處理**
  - 確定被猜中之帳號，並將該帳號停用
  - 刪除Mail Queue之待寄信件(可能刪到正常寄件之信件)

電子郵件安全換證課程 28

- 當密碼被猜中後
  - ✓ 電子郵件系統會出現的問題狀況：
    大量信件寄出、收到大量退信、或Mail Queue中有大量待寄信件，導致電子郵件系統無法正常運作。甚至被列為寄件黑名單，導致無法正常寄信到其他機關。
  - ✓ 建議之緊急處理方案：
    透過郵件稽核紀錄及統計報表找出被猜中之帳號並將該帳號停用。

    刪除Mail Queue之待寄信件(可能刪到正常寄件之信件)。
    若被列入黑名單後，於排除問題後申請黑名單之移除，或者將寄件IP更改為其他IP位址。

電子郵件系統被駭：案例與醒思(1/2)

- 國際貿易雙方以電匯交付貨款，並以電子郵件聯繫
  - 駭客假造電子郵件，使客戶匯款至駭客的帳戶
- 駭客駭進企業的電子郵件系統
  - 直接以企業的名義與客戶聯絡匯款至指定帳戶
- 駭客攔截電子郵件
  - 竄改內容之後寄給客戶
- 郵件炸彈(e-mail bomb)
  - 網路上有這一類的程式可供下載利用

- 一般使用者應該要保持良好的使用習慣與警覺性：
  - ✓ 使用者應盡量使用安全性高的電子郵件密碼，防止帳號被盜用。
  - ✓ 對於重要的電子郵件，應該詳細檢查郵件的真偽。
  - ✓ 進行像匯款的操作時，應該透過多種管道確認，並留意帳戶是否有改變。
- 後面的單元將介紹個種協助我們防護電子郵件使用安全的技術：
  - ✓ 對於偽造的郵件，可以透過**鑑別防偽的機制**來防制。
  - ✓ 若郵件之帳密被駭，可以利用**電子簽章的技術**來達到不可否認性的安全保障，確認寄件者身份。
  - ✓ 預防郵件被攔截，可以**對郵件內容及附檔進行加密**。
- 郵件炸彈(e-mail bomb)是一種程式碼，在執行時會向同一個位址傳送大量郵件，目的是耗盡磁碟空間或使電子郵件或 Web mail伺服器超載，或是使收信的個人遭遇困擾。 電子郵件系統可以透過**郵件連線與內容過濾的功能或是發送行為分析**來偵測。

電子郵件系統被駭：案例與醒思(2/2)

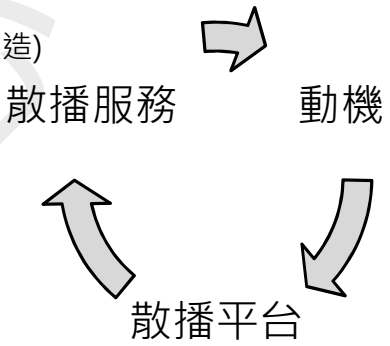
- 多種**勒索軟體**結合社交工程或是APT的攻擊，誘騙受害者，造成資料或是金錢上的損害
- **遠端變更已收到郵件內容**的Ropemaker攻擊
- 民國106年8月資訊專家發現，全球有高達7.1億個電子郵件帳號，遭一隻電郵機器人「利用」，散布含有銀行木馬程式的垃圾郵件
  - 曾被鎖定的電子郵件帳號，應馬上變更密碼
  - 可能連帶造成使用的臉書等其他社交軟體被駭
  - 建議開啟雙重驗證功能

- 勒索軟體、社交工程或是APT的攻擊，是以人性的弱點來達成攻擊的效果，所以在安全防護上一定要建立資安的警覺與素養。
- 英國的電子郵件管理業者Mimecast於106年8月22日揭露了Ropemaker郵件攻擊手法，允許駭客自遠端變更使用者已收到的郵件內容，例如以惡意連結置換原本的連結，或是竄改郵件中的文字。Ropemaker利用了CSS可分離內容與格式的特性，一個CSS檔案可能存放在本地端或是遠端，想像若有駭客傳送一個基於遠端CSS的郵件到受害者信箱中，原本的信件內容是無害的，已通過郵件或企業的安全檢測，但卻可在郵件抵達之後，藉由遠端CSS改變郵件所呈現的內容。
- 民國99年1月Google表示，由於全球中國人權人士的Gmail帳戶遭受源自中國的大規模攻擊，Google檢討大陸營運的可行性，並且準備不惜全面退出中國，後來導致Google退出大陸市場。由此案例可以發現資安的問題也經常與政治問題糾葛在一起，使影響的層面擴大。
- 可以上https://haveibeenpwned.com/，再輸入自己的電子

郵件帳號，即可得知密碼是否被竊取，這個網站蒐集並列出各次惡意攻擊行為，曾被鎖定的電子郵件帳號，如果發現自己的帳號在名單裡，應馬上變更密碼。

透過電子郵件散佈假新聞

- 以誤導的資訊來操縱大眾
- 具有可辨識的特性
- 應採取行動端正視聽
- **常見案例**：
  - 著名周刊報導市售鮮奶驗出禁藥(未查證)
  - 總統大選的出口民調(誤導性質)
  - 大地震之後預警有第二次更大的地震(假造)



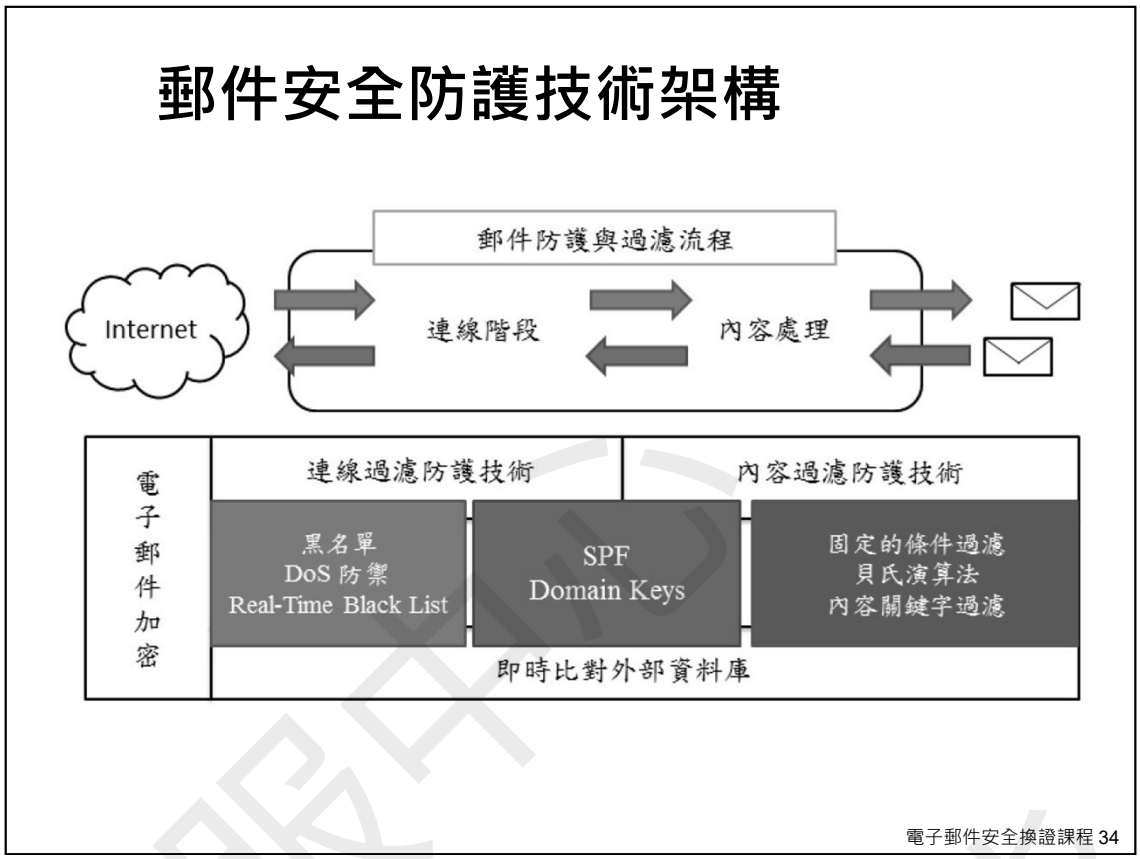
電子郵件安全換證課程 31

- 騙取點擊率的標題、可疑的網域名稱、內容未標示發佈者姓名或日期，或沒標註引用來源等都是假新聞可能具有的特徵。
- 一般人應該勇於熱心採取行動端正視聽。
- 除此之外，在社交工程的攻擊中誤點內容連結時，也應該勇於舉報，避免損害擴大。

第2單元
電子郵件安全防護

單元學習目標

- 熟悉連線過濾、簽章加密、鑑別防偽、內容的過濾、發送行為分析
- 熟悉電子郵件安全管理制度



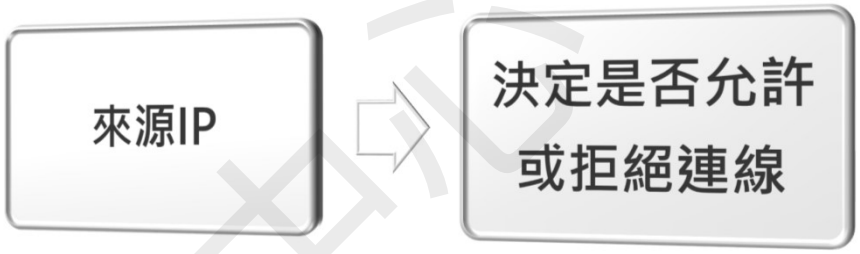
- 有關於電子郵件郵件安全防護技術架構的內容可參考「 電子郵件安全參考指引」

電子郵件伺服器的基本安全控制設定

- 電子郵件伺服器的狀態
- SMTP 、 ESMTP 、 IMAP 、 POP3 、 LDAP 與 SSL/TLS設定
- 垃圾信防治設定、防毒軟體整合設定
- 使用者帳戶設定與管理
- 監控(收發紀錄、系統狀態、事件檢視)
- 過濾(規則設定)
- 安全(IP連線與來源安全、IP白名單、網域黑名單)
- 維護(軟體版本、授權人數)

使用來源IP控管對MTA的連線

- MTA直接以連線封包中的來源IP位址來決定是否允許或拒絕連線(類似防火牆功能)
  - 注意：一般需要開放所有外部IP都可以寄信進來，只拒絕特定黑名單的來源



電子郵件安全換證課程 36

- 用來源IP控管對MTA的連線
- 電子郵件安全防護中最簡單防護就是「來源IP的連線控」，也就是你可以允許哪一些IP可以進行連線，而那些特定IP不允許。
- 但是一般機關的**外部電子郵件伺服器**通常是必須開放外部網際網路所有IP可以連線，因為無法事先確認有那些IP才會寄信到機關的電子郵件伺服器。除非機關掌握特定IP是有問題的，機關可以在電子郵件伺服器上將有問題的來源IP進行阻擋。但並不是所有電子郵件伺服器都支援使用IP來阻擋SMTP連線的功能，所以有可能需要藉由防火牆的存取連線控管來達到阻擋特定IP的連線功能。

使用DNS反解來控管MTA連線

- **進行DNS反解檢查的時機**
  - –連線時：
    - 來源IP的PTR紀錄「是否存在？」
    - 來源IP反解所得的名稱再做正解後是否與來源IP一致？
  - –HELO/EHLO domain時：
    - 檢查「domain 是否存在？」
    - 檢查「domain與來源IP的PTR紀錄是否符合？」
  - –MAIL FROM: user@domain 時：
    - 檢查「domain 是否存在？」
    - 檢查「domain與來源IP的PTR紀錄是否符合？」

- 用DNS反解來控管MTA的連線
- DNS的反解可以用來判斷「傳送來源是否偽冒郵件地址」，藉以判斷是否為可信賴來源，並決定是否接收來信。來源IP的反解若與SMTP HELO及MAIL FROM在相同網域中時，就代表寄件來源沒有偽冒郵件地址的狀況。下列為MTA可以透過DNS反解進行檢查的時機：
  - ✓ 連線時：
    當SMTP的TCP的3方交握一完成，MTA即可取得來源IP的位址。可以檢查來源IP的PTR紀錄「是否存在？」來決定是否允許存取？來源IP反解(IP解析成名稱)所得的名稱再做正解(名稱解析成IP)後是否一致？
  - ✓ HELO/EHLO domain時：
    檢查HELO指令後的「domain 是否存在？」，來決定是否允許存取？檢查HELO指令後「domain與來源IP的PTR紀錄是否符合？」
  - ✓ MAIL FROM: user@domain 時：

檢查MAIL FROM指令中的「domain 是否存在？」，來決定是否允許存取？檢查MAIL FROM指令中的「domain與來源IP的PTR紀錄是否符合？」

- ✓ 基本上DNS的反解可以取得連線來源機器的名稱，MTA透過這個名稱來判斷在SMTP連線中的HELO或MAIL FROM指定中所「宣稱」的domain是否一致？來決定寄件者是否可以信賴？

- **注意1：若垃圾郵件發信人(Spammer)是使用自己的網域來發信，那麼DNS反解無法控管這類狀況。**
- **注意2：當來信端沒有設定好其自己的DNS反解時，有可能導致收不到正常的信件。**

RBL黑名單資料庫

- RBL全名為Realtime Blackhole List
- RBL集中蒐集的黑名單包含
  - –IP位址(Open Relay、被發現發送垃圾信件的主機)
  - –未註冊的DNS網域名稱
  - –電子郵件地址
- 使用RBL要注意的事項
  - –RBL的提供者是否持續更新其黑名單的內容

- RBL黑名單資料庫
- RBL全名為Realtime Blackhole List，通常由廠商或一些公正的第三方蒐集全世界中有那些IP、網域名稱或電子郵件地址，是寄送垃圾信件或惡意信件的來源。在電子郵件伺服器中必須要額外開啟這種黑名單存取控管機制。其運作方式為：當MTA收到信件時，會自動將來源IP送給RBL的提供者進行確認，RBL提供者會立即回應一個狀態碼來告知MTA寄件來源IP是否列在其黑名單中？
- 在選用RBL存取控管時一定要選擇有經常更新RBL的提供者，以確保RBL的內容是正確即時的。

Graylist灰名單過濾機制

- 一般垃圾信件寄送者(spammer) 所用的MTA，寄信之後就不管收信端MTA是否收到它所寄的信
- 相反的，標準的MTA如果寄信之後發生錯誤，會繼續的寄這封信，直到收信端MTA收到這一封信
- **Graylist過濾垃圾信件的方法**
  - 第一次收到郵件就先拒絕這封郵件
  - 等一段時間之後，如果又收到同樣的郵件就接收這封郵件
  - 看起來很簡單的方法，但是按照測試的結果Graylist 可以攔截95%的垃圾信件，剩餘的5%就給更進階的過濾機制來處理
- **採用Graylist的缺點：信件會被延遲寄到**

電子郵件安全換證課程 39

- Graylist灰名單過濾機制
- 一般垃圾信件寄送者(spammer) 所用的 MTA ，因寄件效能的考量，寄信之後就不管收信端MTA是否收到它所寄的信。相反的，標準的MTA 如果寄信之後發生錯誤，它會在隔數分鐘或數小時後繼續的寄這封信，直到收信端MTA收到這一封信。Graylist灰名單運作便是運用這個差異來判斷寄件者是否為垃圾信件的寄送者。
- Graylist過濾垃圾信件的方法如下：
  1. 第一次收到郵件就先拒絕這封郵件。
  2. 等一段時間之後， 如果又收到同樣的郵件就接收這封郵件。
  3. 看起來很簡單的方法，但是按照測試的結果Graylist 可以攔截 95% 的垃圾信件，剩餘的 5% 就給更進階的過濾機制來處理。
- 注意：使用Graylist機制的唯一缺點就是信件會被「延遲」寄到的問題，這個延遲有可能是數分鐘，也有可能是數小時，依寄送端的設定而有差異。

SMTP 使用TLS加密傳輸

- TLS(Transport Layer Security)
- SMTP Client與Server間私密及鑑別的通訊協定
  - 可包含MUA-MTA與MTA-MTA間
  - 無法滿足End to End的加密
- 在ESMTP中定義 STARTTLS 指令
- 不需要任何參數設定
- Server 用來告訴 Client 是否可以用TLS加密傳輸
- 由Client決定是否啟動TLS

- SMTP 使用TLS加密傳輸
- 在ESMTP協定中增加了一個新功能為STARTTLS，可以告訴寄件端MTA或MUA，收件端MTA可以支援TLS的加密傳輸功能，讓信件於傳輸過程中可以確保信件資料的機密性。
- TLS(Transport Layer Security)其實就是IETF將SSL標準化後所定義的名稱，所以TLS 1.0 可以說就等於SSL 3.0。
- SMTP Client與Server間私密及鑑別的通訊協定，可以應用在「MUA與MTA」及「MTA與MTA」間之加密通訊。儘管STARTTLS可以支援ESMTP之加密通訊機制，但卻無法滿足End to End的加密。因為在信件轉送過程中無法保證每一段的傳送一定會被加密，而且信件在儲存時也無加密。STARTTLS指令不需要任何參數，是由MTA Server端告訴MTA Client是否可以用TLS加密傳輸，但由MTA Client端來決定是否啟動TLS。

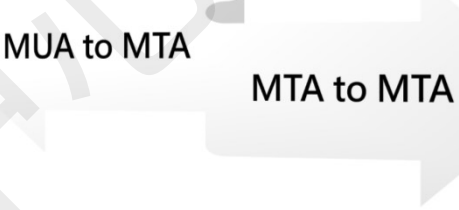
POP3、IMAP4使用SSL加密傳輸

- SSL(Secure Socket Layer)最早是在1994年由網景公司所設計研發而成
- 採用公開金鑰技術
- SSL的協定基本特性：
  - 機密性：在**交握協定(handshake)**定義通訊密鑰後，所有的消息都被加密
  - 身分鑑別：採用點對點之間的身分鑑別，以非對稱式密碼之公鑰(含憑證)之鑑別來確認連線雙方的身分
  - 可靠性：訊息的傳送，使用訊息確認碼(MAC)來確保傳送資訊的完整性

- POP3、IMAP4使用SSL加密傳輸
- SSL(Secure Socket Layer)最早是在1994年由網景公司所設計研發而成，主要應用在Web伺服器與瀏覽器間的身份鑑別與加密通訊，基本上是採用公開金鑰加解密與身份鑑別技術。
  - ✓ SSL的協定基本特性：可以達到通訊的機密性、身分鑑別及可靠性的要求。
  - ✓ 機密性：在交握協定(handshake)定義了通訊密鑰後，所有的消息都被加密。
  - ✓ 身分鑑別：採用點對點之間的身分鑑別，以非對稱式密碼之公鑰(含憑證)之鑑別來確認連線雙方的身分。
  - ✓ 可靠性：訊息的傳送，使用訊息確認碼(MAC)來確保傳送資訊的完整性。

SMTP的來源身分鑑別

- **SMTP使用者身分鑑別(MUA to MTA)**
  - 時機：外勤人員需要透過機關的MTA寄信時使用
  - 採用ESMTP的AUTH LOGIN指令
- **SMTP來源身分鑑別(MTA to MTA)**
  - PTR
  - SPF
  - SenderID
  - DomainKeys
  - DMARC



- SMTP的來源身分鑑別
- SMTP的身份鑑別可以區分為兩部份來談，首先是MUA寄信時MTA要求進行使用者的身份鑑別，這是透過ESMTP協定中的AUTH LOGIN指令來達成，其次為MTA與MTA間的寄信件身份鑑別機制，必須透過其他方法如：PTR、SPF、SenderID或DomainKey等來驗證寄件來源是否可以信賴。

結合SPF與DKIM的DMARC

- DMARC是Domain-based Message Authentication, Reporting and Conformance)的縮寫
- 是一套以SPF及DKIM為基礎的電子郵件認證機制
- 可檢測及防止偽冒身份、防制網路釣魚或垃圾電子郵件

- DMARC是一套以SPF及DKIM為基礎的電子郵件認證機制。可檢測及防止偽冒身份、防制網路釣魚或垃圾電子郵件。

郵件遞送識別機制整理與比較(1/2)

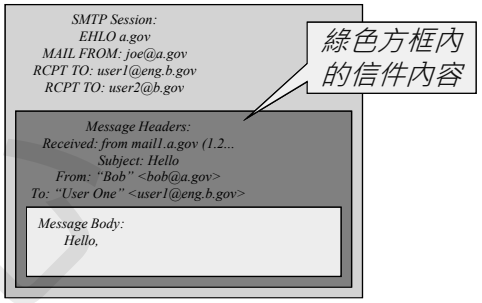
識別機制	運作原理	優點	可能問題
SPF	係透過DNS記錄A機關所擁有之網域，僅可由哪些郵件伺服器寄送郵件；收件方之郵件伺服器會先去查詢DNS以識別來源寄件者的真實性	可藉此判斷寄件者的真偽，避免偽冒寄信行為	此機制之識別與否係由收件方決定，與寄件方無直接關係。若收件方郵件伺服器未有此項功能或未開啟相關機制，則無法有效識別郵件來源之真偽
DKIM	此係產生網域金鑰，寄信時會使用不公開的網域金鑰對信件標頭進行加密，並將可公開的網域金鑰放置於DNS記錄中，讓收件方依據該金鑰進行解密以確認寄件者地址的真偽	可藉此判斷寄件者的真偽，避免偽冒寄信行為	此機制之識別與否係由收件方決定，與寄件方無直接關係。若收件方郵件伺服器未有此項功能或未開啟相關機制，則無法有效識別郵件來源之真偽

郵件遞送識別機制整理與比較(2/2)

識別機制	運作原理	優點	可能問題
閘道式憑證數位簽章	即郵件在寄送時，由郵件伺服器或郵件閘道設備對該封郵件進行數位簽章，數位簽章之簽發憑證為主機或機關所擁有。收信時再由收信軟體去辨識該封郵件所含之數位簽章真偽來識別寄件來源之真偽	不需由個人或寫信軟體去安裝數位簽章機制，不容易受到個人電腦或個人使用環境之干擾	由於數位簽章識別仍需仰賴收件軟體之驗證機制，故會受限個人使用環境或載具限制而影響
個人憑證數位簽章	郵件寄送時即由個人所持有之數位憑證進行簽章；收信時再由收信軟體去辨識該封郵件所含之數位簽章真偽來識別寄件來源之真偽	故會受到個人或寫信軟體對於數位簽章機制的支援性之干擾	由於數位簽章識別仍需仰賴收件軟體之驗證機制，故會受限個人使用環境或載具限制而影響

電子郵件內容過濾

- 針對電子郵件內容(SMTP DATA後的資料)進行審查及過濾的技術
- 內容過濾技術可以偵測：
  - 垃圾郵件
  - 釣魚詐騙郵件(Phishing)
  - 病毒信件
- 內容過濾技術可分為
  - 特徵行為
  - 內容關鍵字
  - 貝式過濾
  - 外部資料庫比對
  - 圖片識別過濾
  - 電子郵件信譽評等



- 電子郵件內容過濾

- 從電子郵件的封裝層次來看，電子郵件內容過濾技術主要是檢查SMTP協定中DATA指令中的內容。這些信件內容過濾技術可以檢查「垃圾郵件」、「釣魚詐騙郵件(Phishing)」、「病毒信件」等，藏在信件內容中的惡意郵件。常見的電子郵件內容過濾技術包含如下：

  - ✓ 特徵行為：透過特定信件內容之特徵及條件來判斷是否為惡意郵件的技術，例如：同一來源發送多封相同主旨的信件時。
  - ✓ 內容關鍵字：透過關鍵字，如：特價、折扣等關鍵字來判斷是否為惡意郵件的技術。
  - ✓ 貝式過濾：透過貝式演算法來學習信件內容的技術。
  - ✓ 外部資料庫比對：透過外部公用的信件內容資料庫，來比對信件內容是否為垃圾信件的技術。
  - ✓ 圖片識別過濾：為避免垃圾信件寄件者透過圖片內容來迴避文字

內容的檢查技術，因此透過OCR技術來識別圖片中的文字內容。

- ✓ 電子郵件信譽評等：依實際檢測到的威脅程度來動態評估寄件者或信件內容信譽的判斷技術。

固定規則式過濾

- 由廠商或國際各使用社群之收集，可能歸納出垃圾郵件的某種規則
- 例如特定寄件者、特定主旨或特定主旨樣式、信件內容中固定的關鍵字句、含有特定網址等
- 多數系統亦支援交叉的條件並以權重方式計分
- 通常規則式過濾會搭配**正規表示式(Regular Expression)**，以有效阻絕規則性推演之垃圾郵件

- 由廠商或國際各使用社群之收集，可能歸納出垃圾郵件的某種規則，例如特定寄件者、特定主旨或特定主旨樣式、信件內容中固定的關鍵字句、含有特定網址等，單純的規則過濾例如黑名單或白名單，只要內容如寄件人名稱、信件主旨、各標頭或信件內容與附檔中符合指定的條件，即判斷信件屬於廣告或正常信；同時多數系統亦支援交叉的條件並以權重方式計分，例如：某主旨跟內文含有某類字句同時成立的話，屬於廣告信的機率就比較高。通常規則式過濾會搭配正規表式(Regular Expression)，以有效阻絕規則性推演之垃圾郵件。

特徵行為過濾

- 大部分的垃圾/廣告郵件可以透過固定式的條件來過濾
- 過濾條件範例：
  - 同一來源發送多封相同主旨的信件(100)
  - 同一來源發送多封內容相似的信件(100)
  - 如果信件中引用外部圖形檔超過3個時(50)
  - 如果信件中含有2個以上的連結時(30)
- 當符合的條件總與超出指定數值(例：60)時就視為垃圾郵件
  - 如果郵件內容只符合第4項規則時，視為正常信件
  - 當郵件內容同時符合第3、4項規則時(50+30=80)，即視為垃圾郵件

- 特徵行為過濾
- 透過特定信件內容之特徵及條件來判斷是否為惡意郵件的技術，基本上大部分的垃圾/廣告郵件都可以透過固定式的條件來過濾，例如：下列為判斷是否為垃圾郵件的條件及其分數，分數愈高代表愈有可能是垃圾郵件。
  1. 發現「同一來源發送多封相同主旨的信件」時可能為垃圾郵件的分數給100分。
  2. 發現「同一來源發送多封內容相似的信件」時可能為垃圾郵件的分數給100分。
  3. 但如果發現「信件中引用外部圖形檔超過3個」時可能為垃圾郵件的分數只給50分。
  4. 如果發現「信件中含有2個以上的連結」時可能為垃圾郵件的分數只給30分。
- 一封信件可能同時符合上述一個或多個條件，可設定當符合的條件分數總與超出指定數值(例：60)時就視為垃圾郵件，例如：
  - ✓ 如果郵件內容只符合第4項規則時，視為正常信件。因為分數

只有30分未達指定的60分。

- ✓ 當郵件內容同時符合第3、4項規則時(分數總合為50+30=80)，超出指定的60分時，即視為垃圾郵件。

內容關鍵字過濾

- 在電子郵件內容中透過關鍵字出現的次數或組合來判斷是否為垃圾郵件的技術
- 關鍵字範例
  - 優惠、折扣、促銷、週年慶
  - 現金卡、貸款、利息、周轉、卡債、低利
- 關鍵字技術
  - 郵件內文全文檢索速度及效能
  - 是否包含附件中的內容
  - 是否可支援多國語系及字元碼(繁簡中文字)
  - 關鍵字同義/同音字(體、体)(馬英九、馬總統英九)
- 關鍵字出現的頻率與次數通常也會納入特徵行為過濾的積分計算
- 透過關鍵字過濾技術可以比對信件中是否包含「個人資料」

- 內容關鍵字過濾
- 在電子郵件內容中透過關鍵字出現的次數或組合來判斷是否為垃圾郵件的技術。常見的關鍵字例如：優惠、折扣、促銷、週年慶、現金卡、貸款、利息、周轉、卡債、低利等。機關可依其特性設定特定的關鍵字以判斷信件中是否包含機關相關的機敏資訊。
- 在選用內容關鍵字過濾技術時，應特別注意下列事項：
  - ✓ 郵件內文全文檢索速度及效能：關鍵字比對經常會依賴全文檢索的技術來提升檢索效能。
  - ✓ 是否包含附件中的內容：由於附件的檔案格式非常多樣，關鍵字過濾技術是否能針對附件檔案內容檢索能力也是評估的關鍵。
  - ✓ 是否可支援多國語系及字元碼(繁簡中文字)：國外產品不見得能支援中文化關鍵字的全文檢索，甚至多國語言的全文檢索。
  - ✓ 關鍵字同義/同音字(體、体)(馬英九、馬總統英九)：關鍵字比對能否區分出中文特有的同音或同義字。
- 內容關鍵字出現的頻率及次數通常也會納入特徵行為過濾的積分計算。

統計方式自動學習分類

- 許多郵件系統或雲端郵件服務提供郵件分類服務，甚至能替使用者將正常信件先分類為不同用途，將類似垃圾郵件的信件細分為商品廣告、電子報或惡意信件等
- 此類技術的特色在於**需要一定的訓練樣本**，而且樣本範圍愈接近使用者實際的信件愈準確
- 即使郵件廠商提供初始的資料庫，仍需再透過時間及資料的累積，才能讓自動分類機制提供使用者滿意的結果

- 許多郵件系統或雲端郵件服務更提供了進一步的郵件分類服務，甚至能替使用者將正常信件先分類為不同用途，將類似垃圾郵件的信件細分為商品廣告、電子報或惡意信件等。此類技術的特色在於需要一定的訓練樣本，而且樣本範圍愈接近使用者實際的信件愈準確。因此即使郵件廠商提供初始的資料庫，仍需再透過時間及資料的累積，才能讓自動分類機制提供使用者滿意的結果。

貝氏過濾(1/2)

- 貝氏定理是結合**「事前機率與條件機率」**，導出「事後機率」的過程
- 運作案例
  - 例如：信件中出現「未滿十八歲」字眼即可能為垃圾信件。如果這封信件同時出現「極品」、「熟女」、「偷拍」等字眼，我們便已幾乎肯定此即為不折不扣的垃圾信件
  - 貝氏過濾法即是採用類似，但更客觀的統計方式來偵測其為垃圾信件之機率
- 投入垃圾郵件及非垃圾郵件，分別交予貝氏過濾之演算法進行訓練

- 貝氏過濾
  - ✓ 貝式過濾法是一個比較聰明的機制，它不需要做關鍵字或是條件的設定。貝式過濾法是一個結合「事前機率」與「條件機率」導出「事後機率」的過程。例如：事前準備了一百封的垃圾信件，這些垃圾信件需要有多樣化的特質，也就是可以代表大部分垃圾信件的特質。經過貝式演算法從這一百封裡面去找出垃圾信到底有甚麼樣的特徵，就可以代表它是一個垃圾信件，這個就叫做事前的機率。之後只要以後任何一封信件進來，就一樣照相同的方法來計算其事後機率是否與事前機率吻合，來決定該封信件是不是垃圾信件。當然貝氏過濾的演算法也必須學習「非」垃圾信件，以判斷什麼樣特徵的信件為正常信件。
  - ✓ 基本上貝式運算法的運作模式下，提供的信件樣本越準、越多，事後的誤判的機會就會越低。再加上垃圾信件樣本隨環境的改變會跟著變動，所以事前樣本的學習應定期執行，以確保樣本的準確率。以下為貝氏過濾的運作案例說明：
  - ✓ 例如：信件中出現「未滿十八歲」字眼即可能為垃圾信件。如果這封信件同時出現「極品」、「熟女」、「偷拍」等字眼，我們

便已幾乎肯定此即為不折不扣的垃圾信件，貝氏過濾法即是採用類似，但更客觀的統計方式來偵測其為垃圾信件之機率。

貝氏過濾(2/2)

- 產生適當的機率規則自動分辨出垃圾郵件與正常郵件
- 投入分析的郵件樣本量越大且越接近現況，此演算法的準確度就越高
- 必須**定期以新樣本進行訓練**才能維持成效

外部資料庫比對

- 外部資料庫是由第三方蒐集整理垃圾信件指紋特徵並分享更新給垃圾信件防護機制使用，來阻擋垃圾信件的傳播
- 目前常見的外部資料庫：
  - DCC
  - Razor
  - Pyzor
    - 與Razor類似，發展初期為Razor的Python實作，後來使用了不同的協定而分道揚鑣

- 外部資料庫比對
- 外部資料庫是由第三方蒐集整理垃圾信件內容的「指紋特徵」並分享更新給垃圾信件防護機制使用，來阻擋垃圾信件的傳播，所謂「指紋特徵」通常是指信件內容的雜湊值，所以不論信件內容大小，其指紋特徵值都很小，易於傳輸及儲放。目前常見的外部資料庫有下列三種：
  - ✓ DCC
  - ✓ Razor
  - ✓ Pyzor

電子郵件過濾規則設定原則

- 黑名單(RBL)寄件來源
- 無法證明來源之寄件者
  - DNS PTR、SPF、DKIM等
- 信件傳送頻率
  - 同一來源寄大量信件
  - 同一主旨寄給多人
- 特定關鍵字
  - 銷售類
  - 情色類

- 電子郵件過濾規則設定原則
- 電子郵件過濾規則設定可依下列原則來訂定，但過濾規則仍應考慮機關需求來訂定之：
  - ✓ 黑名單(RBL)寄件來源：優先參考被列入黑名單的寄件來源，阻擋由黑名單寄出之信件。
  - ✓ 無法證明來源之寄件者：參考DNS PTR、SPF、DKIM等寄件來源鑑別技術，若寄件者有明確的SPF及DKIM宣告，可依其宣告之內容來決定是否為可信賴來源。
  - ✓ 信件傳送頻率：若同一來源寄大量信件或同一主旨寄給多人時應為垃圾信件。
  - ✓ 特定關鍵字：例如：銷售類或情色類等。

電子郵件發送行為分析

- **目的**
  - –從電子郵件的內容或紀錄中找出惡意不當的行為以阻絕攻擊來源
- **對象**
  - –分析電子郵件的標頭(Mail Header)
  - –分析電子郵件伺服器紀錄(Audit Log)
- **電子郵件管理者應定期分析電子郵件系統紀錄以發現異常行為**

- 電子郵件發送行為分析
- 其目的是希望管理者可以定期或不定期從電子郵件的內容或紀錄中找出惡意不當的行為，以阻絕攻擊來源。而發送行為分析的對象區分為分析電子郵件的標頭(Mail Header)及分析電子郵件伺器紀錄(Audit Log)兩大類。電子郵件管理者應定期分析電子郵件系統紀錄以發現異常行為。

分析電子郵件的發送路徑

- **目的**
  - 找出發信來源並進行阻擋或進一步追查
- **方法**
  - 檢視電子郵件的原始內容的「Received:」標頭
- **使用時機**
  - 遭受電子郵件炸彈攻擊時
  - 遭受電子郵件退信攻擊時
  - 若收到假冒身分之郵件時

- 分析電子郵件的發送路徑
- 目的為「找出發信來源」並進行阻擋或進一步追查，通常機關若發生特定異常的電子郵時，若要追查信件的寄送路徑時，可在信件的原始內容中查看「Received:」標頭。一般在遇到下列情況時會使用本方法來追查寄信來源：
  - ✓ 遭受電子郵件炸彈攻擊時。
  - ✓ 遭受電子郵件退信攻擊時。
  - ✓ 若收到假冒身分之郵件時。

寄件人一致性的分析

- **目的**
  - –判斷是否為垃圾/廣告信件的參考依據
  - –判斷是否「可能是」偽冒信件的參考
- **方法**
  - –比對From: 標頭中的domain是否在下列標頭中
    - ➢Received：找出有From:標題的domain發送的
    - ➢Message-ID：找出是由From:標題的domain產生的
  - –比對SMTP的MAIL FROM與From: 標頭
  - –比對SMTP的RCPT TO與To:標頭

- 寄件人一致性的分析
- 一般使用者寄信時，藉由MUA與MTA來組合出相關的信件標頭，在信件標頭中有From:、Received:及Message-ID:等，會標示出寄件來源的網域，通常這些標頭中的資訊應會有一致性及相關性。透過寄件人一致性的分析，可以判斷信件是否為垃圾/廣告信件的，也可以判斷是否「可能是」偽冒信件的參考。
- 比對寄件人一致性的方法如下：
  - ✓ 比對From: 標頭中的doamin是否也出現在Received: 與Message-ID中。
  - ✓ 比對SMTP的MAIL FROM與From: 標頭是否一致。
  - ✓ 比對SMTP的RCPT TO與To:標頭是否一致。

同一帳號或IP持續發信件數過高

- 目的
  - 判斷特定帳號或IP是否被當成垃圾信件的轉信站
- 方法
  - 由電子郵件連線紀錄分析(前10大寄件使用者統計)
  - 由防火牆連線紀錄分析(內部非Mail Server卻有大量SMTP連外的紀錄)

- 同一帳號或IP持續發信件數過高。
- 分析的目的是用來判斷特定帳號或IP是否被當成垃圾信件的轉信站。若有特定的使用者帳號密碼被猜中，隨後機關的郵件伺服器可能就會出現透過該帳號的權限發送大量的信件出去的現象，或者外部特定IP透過機關的MTA發送大量信件給外部的信箱。
- 其分析方法如下：
  - ✓ 由電子郵件連線紀錄分析(前10大寄件使用者統計)。
  - ✓ 由防火牆連線紀錄分析(內部非Mail Server卻有大量SMTP連外的紀錄)。

電子郵件伺服器機密性保護

- 存取控制
  - SMTP、POP3、IMAP4
  - SMTP Relay Control
  - 伺服器管理用連線(Terminal Service /Telnet/SSH)
- 伺服器弱點掃描與修補
  - Mail Server
  - Anti-spam/Anti-virus Server
- 電子郵件傳輸加密
  - SMTP: SSL/TLS
  - POP3, IMAP4: SSL
- 電子郵件本文加密
  - S/MIME 、PGP

- 電子郵件伺服器機密性保護
- 可透過下列保護措施來保護電子郵件伺服器的「機密性」：
  - ✓ 存取控制：透過防火牆的存取控管，只讓授權使用者存取SMTP、POP3、IMAP4服務，開啟MTA的SMTP Relay Control機制，避免任何人使用機關MTA來發送信件，嚴格控管伺服器管理用連線(如：Terminal Service /Telnet/SSH等)。
  - ✓ 定期針對Mail Server及相關防護設備(如：AntiSpam/AntiVirus Server)伺服器進行弱點掃描與弱點修補。
  - ✓ 採用電子郵件傳輸加密的通訊協定，如：SMTP: SSL/TLS、POP3, IMAP4: SSL。
  - ✓ 採用電子郵件本文加密的格式，如：S/MIME 、PGP。

發展郵件安全管理程序注意要點

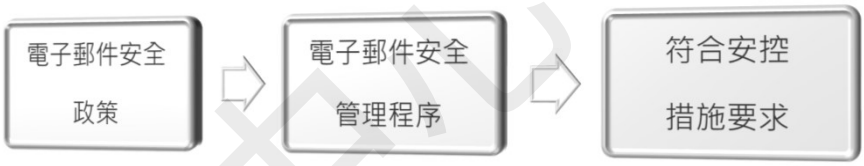
- **為落實執行「電子郵件安全政策」而發展出來的相關管理程序**
  - –電子郵件帳號申請與異動管理程序
  - –電子郵件過濾規則申請與異動管理程序
  - –電子郵件系統變更申請管理程序

電子郵件安全換證課程 60

- 發展郵件安全管理程序注意要點
- 為落實執行「電子郵件安全政策」而發展出來的相關管理程序，常見的電子郵件安全相關控管程序如：
  - ✓ 電子郵件帳號申請與異動管理程序。
  - ✓ 電子郵件過濾規則申請與異動管理程序。
  - ✓ 電子郵件系統變更申請管理程序。

建立相關的郵件安全管理程序

- 郵件帳號申請管理之程序
- 郵件過濾管理之程序範例
- 系統安裝設定之程序
- 改善郵件安全部署架構之程序



- 為落實執行「電子郵件安全政策」而發展出來的相關管理程序，常見的電子郵件安全相關控管程序如(屬於PDCA的Plan)：
  - ✓ 電子郵件帳號申請與異動管理程序。
  - ✓ 電子郵件過濾規則申請與異動管理程序。
  - ✓ 電子郵件系統變更申請管理程序。
  - ✓ 改善電子郵件安全部署架構之管理程序。

改善郵件安全政策或管理程序

- 定期進行檢核
  - 視機關需要進行定期檢核，建議至少每半年要進行檢核
- 成立固定檢核組織
  - 建議由機關內曾參與制定政策的人員來協助檢核目前的政策
- 因應新威脅與增加安全控制措施
  - 新威脅的發生、技術或實施方式的變動，可能會讓現有的郵件管理政策變得過時而不適用

- 改善郵件安全政策或管理程序(PDCA的Plan)
  - ✓ 定期進行檢核：視機關需要進行定期檢核，建議至少每半年要進行檢核。
  - ✓ 成立固定檢核組織：建議由機關內曾參與制定政策的人員來協助檢核目前的政策。
  - ✓ 因應新威脅與增加安全控制措施：新威脅的發生、技術或實施方

式的變動，可能會讓現有的郵件管理政策變得過時而不適用。

電子郵件系統部署規劃要點(1/2)

- 檢視原來的網路架構
  - 例如：目前網路架構圖、郵件伺服器(Mail Server)、DNS Server、Gateway、路由器(Router)、網路切割等，並準備規劃導入後的架構
- 明確區分出**內部、外部網路**
  - 區分出內部網路與外部網路所提供的服務與管制目的，而對應分配出不同網域中的網路設備
- 盤點網路架構清單
  - 將網路架構及其中所安裝應用系統、伺服器、網路設備標示於架構圖中，並標出對應的IP 位址。都需將IP來源位址、IP 目的位址及使用的通訊埠進行記錄，同時要**制定管制規則**
  - 可運用導入工具【Email 相關系統主機清單】

- 電子郵件系統部署規劃要點(PDCA的Do)
  - ✓ 檢視原來的網路架構：目前的網路架構圖、郵件伺服器(Mail Server)、DNS Server、Gateway、路由器(Router)、網路切割...等，並準備規劃導入後的架構。
  - ✓ 明確區分出內部、外部網路：區分出內部網路與外部網路所提供的服務與管制目的，而對應分配出不同網域中的網路設備。
  - ✓ 盤點網路架構清單：將網路架構及其中所安裝應用系統、伺服器、網路設備標示於架構圖中，並標出對應的IP 位址。都需將IP 來源位址、IP 目的位址及使用通訊埠進行記錄，同時要制定管制規則。可運用電子郵件安全參考指引附件7「Email 相關系統主機清單」。

電子郵件系統部署規劃要點(2/2)

- 電子郵件伺服器採購時可考慮之安全功能要求
  - 支援Relay Console功能，避免被非授權轉寄信件
  - 支援ESMTP、POP或IMAP標準傳輸加密機制，並與現有Mail用戶端工具(如：Outlook等)相容
  - 支援ESMTP使用者身份鑑別機制
  - 支援DNS PTR、SPF、SenderID等寄件來源身份驗證功能
  - 支援DKIM郵件簽章及驗章機制
  - 內建(或選用)電子郵件防毒及垃圾郵件過濾機制
  - Webmail可支援HTTPS傳輸加密

郵件安全防護的部署原則

- 無論是政府機關及個人都須做好郵件安全防護的部署原則
- 以**個人使用者**而言
  - 須於郵件系統中進行安全性設定
  - 強化 使用郵件的安全
- 以**組織**而言
  - 可根據網路架構及管理需求以部署郵件安全管理系統，又可區分為閘道式與側錄式等類型的部署架構
  - 政府機關可做為設備部署及規劃之參考

- 無論是政府機關及個人都須做好郵件安全防護的部署原則，以個人使用者而言，須於郵件系統中進行安全性設定，以強化 使用郵件的安全。以組織而言，可根據網路架構及管理需求以部署郵件安全管理系統，又可區分為閘道式與側錄式等類型的部署架構，政府機關可做為設備部署及規劃之參考。

郵件匣道系統的評估

- 過濾連線，節省並保護內部網路資源
- 阻擋、標示或隔離廣告信與惡意郵件
- 外寄時過濾機敏資訊並偵測異常狀況

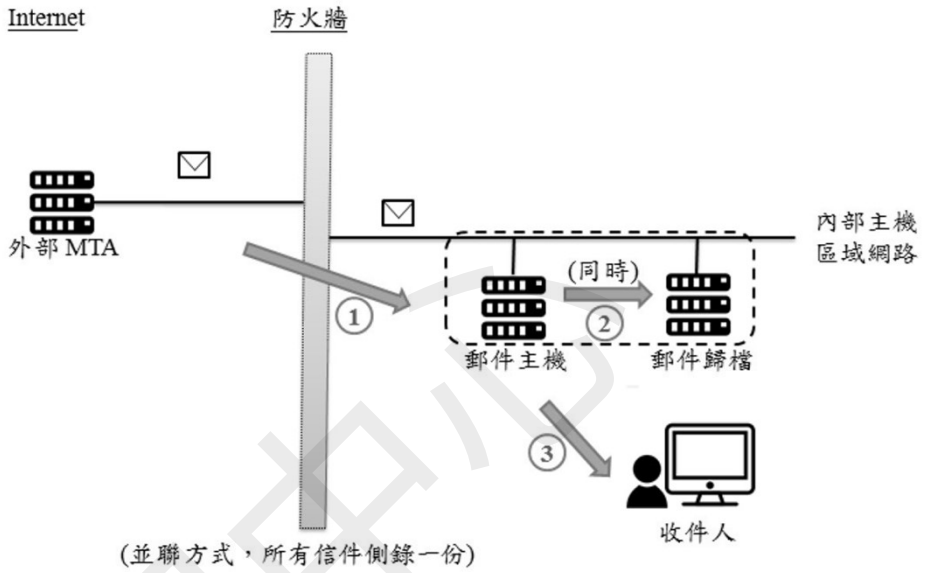
- 郵件的寄送可分為接收及外寄兩個方向，而當要評估郵件匣道系統時，在接收方向，又可以細分過濾連線與郵件內容檢測兩個階段建議具備的功能。

郵件服務品質(Quality of Service, 簡稱QoS)

- 以雲端環境為例
- 內部寄件端
  - 內部指的是整個雲端環境內部
  - 應確保足夠的頻寬，避免用戶外寄大量資料時，佔據所有頻寬，影響自己發送信件的效率與權益
- 外部寄件端
  - 外部是指郵件外寄的接收對象
  - 機關用戶需確認雲端服務供應商或郵件伺服器能否總量控管所有使用者與郵件的寄送狀況，讓郵件發送頻率維持平穩，避免被列入黑名單

- 內部寄件端
  - ✓ 這邊的內部指的是整個雲端環境內部，雲端服務使用者應該要確保自己有使用到足夠的頻寬，避免當有其中之用戶外寄大量資料時，佔據所有頻寬，影響自己發送信件的效率與權益。
- 外部寄件端
  - ✓ 這邊所指的外部，是指郵件外寄的接收對象。一般機關用戶只要同網域中有一個使用者對特定一個郵件服務商，例如像Gmail或Yahoo!，有過於頻繁的郵件發送狀況，就有可能導致該網域整個被該郵件服務商當作威脅來源、進而列入黑名單，導致信件無法寄達，影響事務運作的狀況。機關用戶需確認雲端服務供應商或郵件伺服器能否總量控管所有使用者與郵件的寄送狀況，讓郵件發送頻率維持平穩，避免被列入黑名單。

組織的側錄備份、歸檔與分析



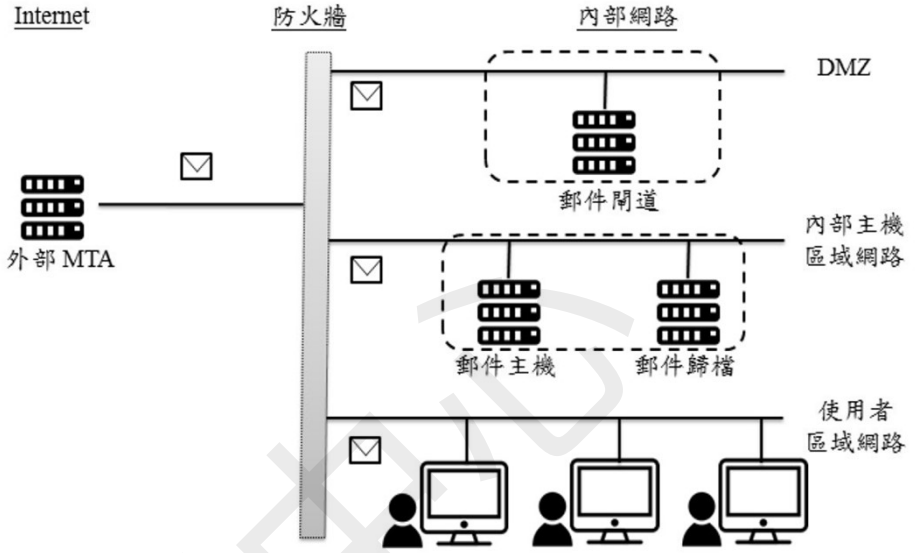
- 郵件側錄機制可比喻為電路並聯，信件會同時提供給郵件主機與郵件側錄系統，給郵件主機的信件就接續一般的流程，繼續遞送給收件人，而同時由側錄系統收到的信件，則可用於備份與歸檔等用途，因此這類郵件側錄系統通常稱為郵件歸檔或郵件備份系統。

側錄機制的資訊安全應用

- 歸檔電子郵件以供調閱與稽核
- 備份電子郵件以便需要時還原
- 分析信件流向及內容偵測異常狀況

- 相對於閘道，側錄機制因為不干涉任一封郵件，而是完整詳實地抄錄所有的電子郵件資料，因此可以忠實地記錄所有軌跡，在系統功能與硬體資源配合的情況下，可以幫助政府機關達成各種資訊安全應用。

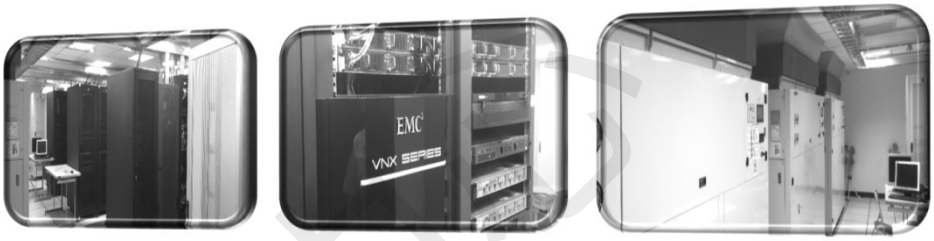
郵件閘道與側錄系統同時部署架構



- 在規劃上也可以採用郵件閘道系統與郵件歸檔側錄系統同時部署的架構，同時取得兩種部署方式的功能。

其他的部署方式與應用

- 封閉式與無害化電子郵件架構
- 複製部分資料以區隔存取行為之架構
- 結合自建主機與雲端服務之混合雲架構

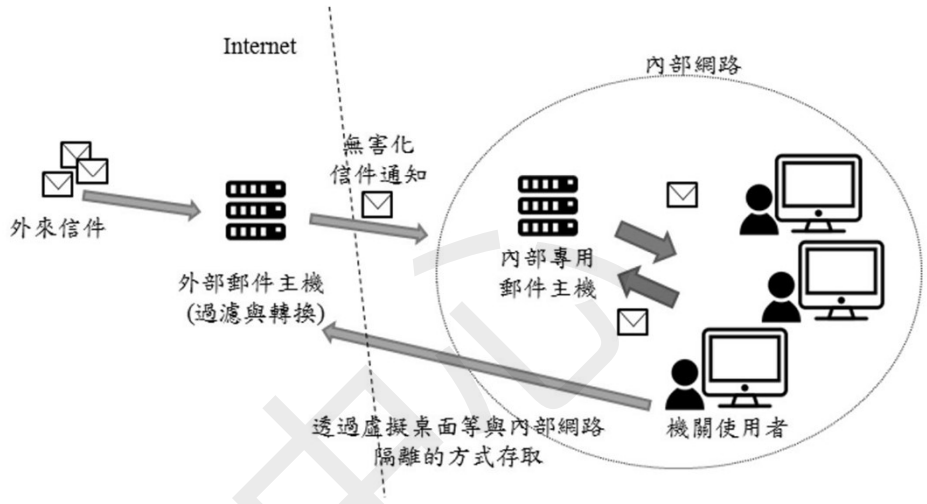


封閉式與無害化　區隔存取行為　混合雲架構

- 封閉式與無害化電子郵件架構
  - ✓ 基於希望內部網路完全純淨無害的原則，又兼顧電子郵件與Internet互通的特性，機關可設計內、外兩套郵件系統以便隔離可能的威脅，讓內部網路保持封閉、無害的電子郵件系統架構。
- 複製部分資料以區隔存取行為之架構
  - ✓ 應用內、外部隔離的郵件主機，機關正式的郵件主機僅提供機關使用者在內部網路收發，如此一來對於郵件主機的保護可以單純化，防火牆僅開放郵件主機對外與其它MTA間SMTP 往來的權限，其餘與該郵件主機的溝通，限於機關內部網路。
- 結合自建主機與雲端服務之混合雲架構
  - ✓ 政府機關欲導入雲端運服務同時，亦可評估混合雲 (Hybrid Cloud) 之架構。運用雲端服務之高可用性、隨時隨處可存取以及動態調整資源之特性之同時，繼續應用原有自建 (On

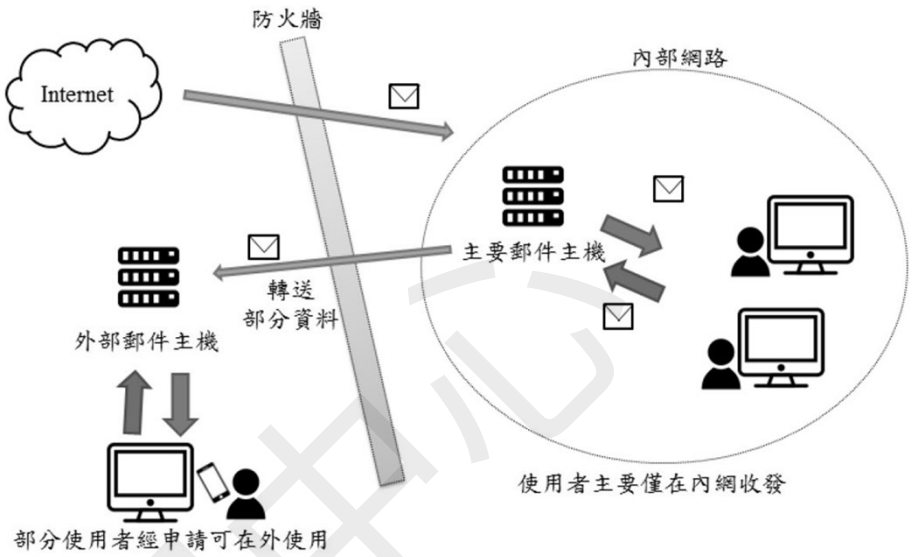
Premises) 之主機設備，兩相結合另可發揮不同的綜效。

封閉式與無害化電子郵件架構



- 基於希望內部網路完全純淨無害的原則，又兼顧電子郵件與Internet互通的特性，機關可設計內、外兩套郵件系統以便隔離可能的威脅，讓內部網路保持封閉、無害的電子郵件系統架構。

複製部分資料區隔存取行為之架構



- 一樣應用內、外部隔離的郵件主機，機關正式的郵件主機僅提供機關使用者在內部網路收發，如此一來對於郵件主機的保護可以單純化，防火牆僅開放郵件主機對外與其它MTA間 SMTP 往來的權限，其餘與該郵件主機的溝通，限於機關內部網路。

結合自建主機與雲端服務之混合雲架構

- 以雲端郵件過濾服務將惡意威脅隔絕在外
- 以雲端服務為備援系統，提升郵件服務整體可用性
- 以混合雲方式異地備份重要資料

- 政府機關欲導入雲端運服務同時，亦可評估混合雲 (Hybrid Cloud) 之架構。運用雲端服務之高可用性、隨時隨處可存取以及動態調整資源之特性之同時，繼續應用原有自建 (On Premises) 之主機設備，兩相結合另可發揮不同的綜效。

系統維護與例行安全檢查(1/2)

- 無論是自行或委外進行郵件伺服器、相關設備的維護作業之注意要點：
  - 參考系統文件進行正確的維護作業
  - 郵件伺服器及相關設備若需進行遠端維護時，須監控這些被授權使用的遠端執行維護與診斷活動
  - 須留存維護作業相關紀錄(包含時間、授權維護者、系統維護動作)，可運用內部資訊系統的時鐘(Time Server)產生稽核紀錄「時戳」(包含日期、時間)，以供後續稽查之用

- 系統維護與例行安全檢查(1/2)
- 無論是自行或委外進行郵件伺服器、相關設備的維護作業之注意要點：
  - ✓ 參考系統文件進行正確的維護作業。
  - ✓ 郵件伺服器及相關設備若需進行遠端維護時，須監控這些被授權使用的遠端執行維護與診斷活動。
  - ✓ 須留存維護作業的相關紀錄(包含時間、授權維護者、系統維護動作)，可運用內部資訊系統的時鐘(Time Server)產生稽核紀錄的「時戳」(包含日期、時間)，以供後續稽查之用。

系統維護與例行安全檢查(2/2)

- 須定期或不定期檢視並分析郵件伺服器及相關設備(如電子郵件安全管理系統)的紀錄檔(Log)，並運用儲存空間不足的檢查機制，以避免超出容量而無法儲存郵件
- 針對郵件系統處理過程中發生錯誤或失敗，可運用自動偵測與警示通知的功能，以即時偵測問題
- 機關進行安全性檢查時，可考慮針對郵件伺服器及相關設備進行系統弱點掃描、病毒掃描、或監測郵件流量，**以察覺是否有異常**

- 系統維護與例行安全檢查(2/2)
  - ✓ 須定期或不定期檢視並分析郵件伺服器及相關設備(如電子郵件安全管理系統)的紀錄檔(Log)，並運用儲存空間不足的檢查機制，以避免超出容量而無法儲存郵件。
  - ✓ 針對郵件系統處理過程中發生錯誤或失敗，可運用自動偵測與警示通知的功能，以即時偵測問題。
  - ✓ 機關進行安全性檢查時，可考慮針對郵件伺服器及相關設備進行系統弱點掃描、病毒掃描、或監測郵件流量，以察覺是否有異常。

系統紀錄/報表檢查要點

- 記錄獲得授權的郵件使用行為
  - 包含：使用者帳號、收發郵件的日期與時間、事件的類型、內容及附加檔案
- 記錄所有特別權限的操作
  - 包含:管理者帳號及主管帳號使用情形
- 記錄未經授權之存取企圖
  - 包含：系統存取動作失敗或被拒絕、違反郵件過濾政策行為與通知、企圖改變系統安全設定與控制
- 留存系統警報或故障之相關紀錄
  - 包含：控制台警報或訊息、系統日誌異常情況、網路管理警報、存取控制系統警報
- 妥善保存及保護管理報表，並測試電子郵件內容及相關系統備份機制之**可用性**與儲存資料的**完整性**

- 系統紀錄/報表檢查要點
  - ✓ 記錄獲得授權的郵件使用行為：包含:使用者帳號、收發郵件的日期與時間、事件類型、內容及附加檔案。
  - ✓ 記錄所有特別權限的操作：包含:管理者帳號及主管帳號使用情形。
  - ✓ 記錄未經授權之存取企圖：包含:系統存取動作失敗或被拒絕、違反郵件過濾政策行為與通知、企圖改變系統安全設定與控制。
  - ✓ 留存系統警報或故障之相關紀錄：包含:控制台警報或訊息、系統日誌異常情況、網路管理警報、存取控制系統警報。
  - ✓ 妥善保存及保護管理報表，並測試電子郵件內容及相關系統備份機制之可用性與儲存資料的完整性。
- 針對系統維護及例行安全檢查時，須注意以下要點：
  - ✓ 須檢查郵件伺服器及相關設備(如電子郵件安全管理系統)系統紀錄中的頻繁錯誤登入紀錄或異常的遠端登入。
  - ✓ 郵件伺服器及相關設備須提供持續監控系統狀態的功能，以協助資訊人員能確認系統的安全設定狀態。

- ✓ 須監控郵件伺服器及相關設備資訊系統的維護狀況，並檢查執行維護的系統紀錄。
- ✓ 對於郵件伺服器及相關設備進行組態變更設定時，須評估此異動造成將產生哪些影響。

建立帳號管理要點

- 制定郵件帳號的使用規則
  - 依據政策制定出郵件使用者的合法使用規則，並描述其使用郵件伺服器或相關設備的使用權責，記載該人員能使用哪些郵件服務(如郵件加密、一般郵件收發服務)
- 制定郵件帳號的個人化服務規則
  - 若電子郵件安全管理系統有提供使用者個人化服務功能，則可加註是否開放使用個人化服務功能
- 區分郵件稽核人員的使用規則
  - 若允許單位主管稽核管轄人員的Email，則加註該主管可使用郵件稽核功能及管轄的群組名稱
- 人員的使用權限劃分，可使用「Email分權管理表」進行相關記載

- 建立帳號管理要點
  - ✓ 制定郵件帳號的使用規則：依據政策制定出郵件使用者的合法使用規則，並描述其使用郵件伺服器或相關設備的使用權責，記載該人員能使用哪些郵件服務(如郵件加密、一般郵件收發服務)。
  - ✓ 制定郵件帳號的個人化服務規則：若電子郵件安全管理系統有提供使用者個人化服務功能，則可加註是否開放使用個人化服務功能。
  - ✓ 區分郵件稽核人員的使用規則：若允許單位主管稽核管轄人員的Email，則加註該主管可使用郵件稽核功能及管轄的群組名稱。
  - ✓ 人員的使用權限劃分，可使用「 Email分權管理表」進行相關記載。

郵件內容安全過濾要點(1/3)

- 維持郵件安全及可用性
  - Inbound 郵件內容(夾帶病毒、惡意程式等威脅及垃圾郵件)
  - Outbound郵件內容(有散播色情文字、圖片、影像、聲音等資訊、發送騷擾他人之郵件內容、發送誹謗電子郵件的危害機關事件)
  - 電子郵件加密或經由加密通道傳送郵件，是無法對此郵件進行過濾
- 運用郵件安全過濾機制
  - 運用電子郵件安控機制、自動化工具及相關稽核程序，以稽查異常行為

- 郵件內容安全過濾要點(1/3)
  - ✓ 維持郵件安全及可用性：
    Inbound 郵件內容(夾帶病毒、惡意程式等威脅及垃圾郵件)。
    Outbound 郵件內容(有散播色情文字、圖片、影像、聲音等資訊、發送騷擾他人之郵件內容、發送誹謗電子郵件的危害機關事件)。
    電子郵件加密或經由加密通道傳送郵件，是無法對此郵件進行過濾。
  - ✓ 運用郵件安全過濾機制：
    運用電子郵件安控機制、自動化工具及相關稽核程序，以稽查異常行為。

郵件內容安全過濾要點(2/3)-病毒與附檔過濾

- 加強病毒交叉防護功能
  - 若機關內部Client 端或其他重要的伺服器已安裝防毒軟體，建議導入閘道式防毒軟體時，**可安裝別於原有品牌的其他防毒產品**，如此同時擁有多家不同的病毒庫，可達到病毒交叉防護的加乘效果
- 維護郵件收發效率
  - 人員透過電子郵件來大量轉寄影音類的大容量檔案(如.mpe 、.asf 、.mov 、.mpeg 、.avi 、.asx 、.mpg 、.wma 、.mp3)
  - 若發送對象過多，將會造成流量阻塞而影響郵件收發效率
- 阻擋HTML惡意電子郵件
  - 以電子郵件的格式而言，純文字檔(Text-based file)是較具安全性的

- 郵件內容安全過濾要點(2/3)- 病毒與附檔過濾
  - ✓ 加強病毒交叉防護功能：若機關內部Client 端或其他重要的伺服器已安裝防毒軟體，建議導入閘道式防毒軟體時，可安裝別於原有品牌的其他防毒產品，如此同時擁有多家不同的病毒庫，可達到病毒交叉防護的加乘效果。
  - ✓ 維護郵件收發效率：人員若透過電子郵件來大量轉寄影音類的大容量檔案(如.mpe 、.asf 、.mov 、.mpeg 、.avi 、.asx 、.mpg 、.wma 、.mp3..等)，若發送對象過多，將會造成流量阻塞而影響郵件收發效率。
  - ✓ 阻擋HTML惡意電子郵件：以電子郵件的格式而言，純文字檔(Text-based file)是較具安全性的。

郵件內容安全過濾要點(3/3)-垃圾郵件過濾

- 擬出良好之過濾政策
  - 垃圾郵件的定義：尤其應對模糊地帶的電子報或私人信件予以定義
  - 組織分工下各部門的過濾策略：以彈性代替單一政策僵化Email的應用
  - 個人化的權限開放：包含整體管理政策與可依個人需要而訂立彈性管理..等政策，都應先明確規範
  - 其他特殊狀況的過濾：制式化往來郵件、以特殊方式寄送的大量郵件等
- 訂定合適之郵件規則
  - 有了良好的郵件過濾策略，才能訂定合適的黑、白名單及各種郵件規則，對於防堵垃圾郵件亦能達到事半功倍的效果

- 郵件內容安全過濾要點(3/3)- 垃圾郵件過濾要求
  - ✓ 擬出良好之過濾政策：
    垃圾郵件的定義：尤其應對模糊地帶的電子報或私人信件予以定義
    組織分工下各部門的過濾策略：以彈性代替單一政策僵化Email的應用
    個人化的權限開放：包含整體管理政策與可依個人需要而訂立彈性管理..等政策，都應先明確規範
    其他特殊狀況的過濾：制式化往來郵件、以特殊方式寄送的大量郵件等
  - ✓ 訂定合適之郵件規則：
    有了良好的郵件過濾策略，才能訂定合適的黑、白名單及各種郵件規則，對於防堵垃圾郵件亦能達到事半功倍的效果

郵件內容備份要點

- 資料保護、稽查與舉證
  - 許多國家已認定電子郵件為法律存證的依據，因應需要做好資料分類與分級，並定義好各類資料的儲存、檢閱、傳送...等相關管理政策
  - 以備日後稽查舉證之需，需利用郵件伺服器與相關設備將郵件內容與系統紀錄進行備份
  - 保護備份資料，以避免遭非授權竄改
- 定期檢查、**測試資料復原程序**
  - 規劃備份機制時，可考慮多元備份方式，視資料重要性進行對應的儲存規劃，定期檢查測試資料回復的程序，以確保回復程序有效且能在指定時間內完成復原作業，才能達到適時分散風險及後續復原的目的

- 郵件內容備份要點
  - ✓ 資料保護、稽查與舉證：
    許多國家已認定電子郵件為法律存證的依據，因應需要做好資料分類與分級，並定義好各類資料的儲存、檢閱、傳送...等相關管理政策。
    以備日後稽查舉證之需，需利用郵件伺服器與相關設備將郵件內容與系統紀錄進行備份。
    保護備份資料，以避免遭非授權竄改。
  - ✓ 定期檢查、測試資料復原程序：
    規劃備份機制時，可考慮多元備份方式，視資料重要性進行對應的儲存規劃，定期檢查測試資料回復程序，以確保回復程序有效且能在指定時間內完成復原作業，才能達到適時分散風險及後續復原的目的。

郵件稽核作業的管理要點(1/2)

- 關於**郵件稽核作業**的管理要點如下：
  - 執行郵件稽查前，須將郵件安全管理政策進行全員公告，並聲明違規罰則
  - 尊重隱私權，並遵循單位的合法偵查程序，才得以偵查違法使用之情節
  - **若未經機關首長或資訊安全長之授權，或非經帳號使用者之同意協助處理故障問題等情形，系統管理人員不得閱讀其他人員的電子郵件內容**
  - 發現若有可疑的網路安全情事，資訊人員得依授權規定執行，使用自動搜尋工具檢查檔案
  - 資訊人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾

電子郵件安全換證課程 83

- 郵件稽核作業的管理要點(1/2)
- 關於郵件稽核作業的管理要點如下：

  - ✓ 執行郵件稽查前，須將郵件安全管理政策進行全員公告，並聲明違規罰則。
  - ✓ 尊重隱私權，並遵循單位的合法偵查程序，才得以偵查違法使用之情節。
  - ✓ 若未經機關首長或資訊安全長之授權，或非經帳號使用者之同意協助處理故障問題..等情形，系統管理人員不得閱讀其他人員的電子郵件內容。
  - ✓ 發現若有可疑的網路安全情事，資訊人員得依授權規定執行，使用自動搜尋工具檢查檔案。
  - ✓ 資訊人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

郵件稽核作業的管理要點(2/2)

- 電腦作業時間應定期校正，以維持系統稽核紀錄的正確性及可信度
- 郵件稽核之需求及查核範圍，應經權責主管人員同意
- 針對事故稽核紀錄定義的保存期限，除了需符合政府相關資安規範以及該機關資訊保存需求外，也**有助於支援資安事故發生後之犯罪偵查與佐證事實**
- 執行電子郵件稽核之系統存取作業，應予監督與留下紀錄，以備日後查考。針對事件稽核紀錄與相對稽核的工具，應落實保護，防止未經授權的存取使用、修改及刪除
- (例如：應限定以唯讀方式存取軟體及資料，若不能以唯讀方式進行系統存取時，應獨立複製另外一份系統檔案供稽核作業之用，且應於稽核作業完成後，立即消除檔案)

- 郵件稽核作業的管理要點(2/2)
  - ✓ 電腦作業時間應定期校正，以維持系統稽核紀錄的正確性及可信度。
  - ✓ 郵件稽核之需求及查核範圍，應經權責主管人員同意。
  - ✓ 針對事故稽核紀錄定義的保存期限，除了需符合政府相關資安規範以及該機關資訊保存需求外，也有助於支援資安事故發生後之犯罪偵查與佐證事實。
  - ✓ 執行電子郵件稽核之系統存取作業，應予監督與留下紀錄，以備日後查考。針對事件稽核紀錄與相對稽核工具，應落實保護，防止未經授權的存取使用、修改及刪除。
  - ✓ (例如：應限定以唯讀方式存取軟體及資料，若不能以唯讀方式進行系統存取時，應獨立複製另外一份系統檔案供稽核作業之用，且應於稽核作業完成後，立即消除檔案。

雲端電子郵件使用安全注意事項

- 應確認電子郵件是在自己同意的情況下由其他人轉寄或分享
- 檢查帳戶是否有異常的使用情形或活動
- 檢查有權存取雲端帳戶資料的服務清單
- 避免使用公用電腦登入雲端帳戶
- 啟用兩步驟驗證(One Time Password, OTP)來強化帳號安全

- 兩步驟驗證已經開始流行，許多大型的網站都支援這個標準。兩步驟驗證的名稱很多，如：兩階驗證、兩階段驗證、動態密碼、一次性密碼、2FA(Two Factor Authentication)、OTP(One Time Password)。所有的概念源自於RFC 6238 TOTP: Time-Based One-Time Password Algorithm與RFC 4226HOTP: An HMAC-Based One-Time Password Algorithm這兩個標準。而現代的大型網站之兩步驟驗證的終端工具，也是實作這些標準而成。
- 兩步驟驗證(2FA, Two Factor Authentication)流程簡述如下：

  1.系統產生一組Key給使用者，並將這組Key存在資料庫內。

  2.使用者從介面上，得到一個「otpauth://totp/{0}?secret={1}」的QRCode。其中的{0}是你的系統名稱(可亂取)，{1}是一個Base32Encode過的Key值。

  3.使用者用Google或Microsoft的驗證器App照這組QRcode，會開始得到一個每30秒跳動一次的動態密碼。

4.使用者回到系統登入頁面，系統會先通過常態性的「帳號密碼」驗證，來得知使用者是誰。

5.得知是哪個使用者後，到資料庫取出該使用者的Key。

6.進行RFC 6238 TOTP運算。

7. 取出UTC制之System.DateTime(1970, 1, 1, 0, 0, 0, System.DateTimeKind.Utc) ~ System.DateTime.UtcNow，取總秒數再去除30秒，即為counter量。

8.進行RFC 4226 HOTP運算。

9. 基礎運算System.Security.Cryptography.HMACSHA1(bytKey[]).ComputeHash(bytCounter[])。

10.移位運算後，取餘數6個數字(不足者左方補0)，得到答案result。

11.將使用者看App後所輸入的密碼，與result進行比對，正確的話就是通過了！

何謂電子郵件社交工程攻擊

- **社交工程**，英文為Social Engineering，是以影響力或說服力來欺騙他人以獲得有用的資訊，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法
- 攻擊者運用的是「人性的弱點」
  - 貪心：撿便宜的個性
  - 好奇：探索八卦訊息的個性
  - 不在意：沒那麼倒楣吧的想法
  - 警覺力：無所謂後果的嚴重性
- 電子郵件社交工程攻擊就是以電子郵件為媒介進行之社交工程攻擊行為

- 何謂電子郵件社交工程攻擊
- 社交工程，英文為Social Engineering，在駭客理論中，指利用人性弱點、利用人際交往上的漏洞，來獲取重要資料的行為。專門指不需要使用任何的程式、科技技術即可獲取帳號、密碼、信用卡密碼、身分證號碼、姓名、地址或其他可確認身分或機密資料的方法。這是近年來造成企業或個人極大威脅與損失的駭客攻擊手法。
- 攻擊者運用的是「人性的弱點」包含有：
  - ✓ 貪心：撿便宜的個性。
  - ✓ 好奇：探索八卦訊息的個性。
  - ✓ 不在意：沒那麼倒楣吧的想法。
  - ✓ 警覺力：無所謂後果的嚴重性。
- 需所謂「電子郵件社交工程攻擊」就是以電子郵件為媒介進行之社交工程攻擊行為。

社交工程的態樣

- 社交工程的態樣是指攻擊的手法與特徵
  - 利用電話佯裝資訊人員，騙取帳號及通行碼偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼
  - 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚
  - 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料
  - 利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、 p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料
  - 利用即時通訊軟體如 MSN ，偽裝親友來訊，誘騙點選來訊中之連結後中毒

- 學員可參考行政院國家資通安全會報網站(http://www.nicst.ey.gov.tw)上的資訊。
- 社交工程 (Social Engineering) 利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。

防治社交工程的方法

- 隨時提高警覺，不未經確認即提供資料
- 不開啟來路不明的電子郵件及附加檔案
- 不連結及登入未經確認的網站
- 不下載非法軟體及檔案

- 社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但能透過下列的方法來防治：
  - ✓ 隨時提高警覺，不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。

垃圾電子郵件詐騙(1/2)

- 通知更新個人資料 (其實是騙局)
- 通知剛剛已更新個人資料 (讓收信者以為帳號被盜)
- 通知郵箱滿了，再不登入處理就會收不到信
- 通知收信者透過提供的連結進行軟體的升級

- 隨著一般人在網路上的活動與關係越來越多元化，駭客有更多的管道與手法來進行詐騙，垃圾電子郵件是十分常見的手段。

垃圾電子郵件詐騙(2/2)

- 通知有不正常的登入活動
- 通知剛完成網路購物
- 通知有優惠活動
- 通知有好友要分享照片和檔案

- 電子郵件的使用者要具備一般的判別要領，在檢視電子郵件時提高警覺。

郵件服務可用性(1/4)

- 資訊安全應顧及機密性、完整性及可用性，三者之中最易被忽略的即為「可用性」
- 若一項資訊服務或資料無法被具有授權且需要使用的人員取用，除了造成機關生產力損失之外，也可能引發其它諸多問題
- 電子郵件系統或雲端郵件服務是否穩定、快速地提供服務，也屬於電子郵件資訊安全中重要的一環

- 資訊安全應顧及機密性、完整性及可用性，三者之中最易被忽略的即為「可用性」，若一項資訊服務或資料無法被具有授權且需要使用的人員取用，除了造成機關的生產力損失之外，也可能引發其它諸多問題。因此電子郵件系統或雲端郵件服務是否穩定、快速地提供服務，也屬於電子郵件資訊安全中重要的一環。

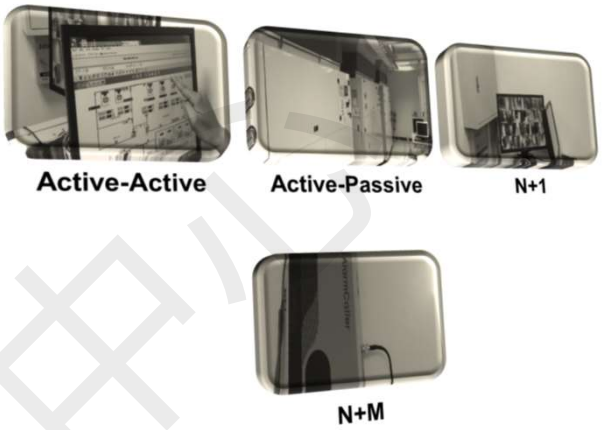
提高資訊服務可用性的做法(2/4)

- 部署足夠的**備援 (Redundant) 設備**，避免各項硬體設備故障導致服務中斷
- 可投注資源避免各環節的單點故障 (Single Point of Failure)
- 從最底層的網路設備，最基本的硬碟，至主機、網路、甚至空調與電力，都有超過基本運作所需的準備，也就是備援措施，即可降低因設備障礙造成的衝擊

- 欲提高資訊服務的可用性，最常見的做法就是部署足夠的**備援** (Redundant) 設備，避免各項硬體設備故障導致服務中斷，可投注資源避免各環節的單點故障 (Single Point of Failure)，從最底層的網路設備，最基本的硬碟，至主機、網路、甚至空調與電力，都有超過基本運作所需的準備，也就是備援措施，即可降低因設備障礙造成的衝擊。

備援方式(3/4)

- Active-Active
- Active-Passive (亦常稱為 Active-Standby)
- N+1
- N+M



電子郵件安全換證課程 93

- 備援方式一般可依即時程度分為Active-Active、Active-Passive (亦常稱為 Active-Standby)、N+1或N+M 等不同模式。
- 在郵件服務的部署中，常會在最前端對外提供各項服務的主機設置Active-Active的機制，例如郵件所必須提供的SMTP、POP3與IMAP4服務，使用Active-Active 方式備援時，應注意其中若部分設備故障時，剩餘的設備是否能承擔全部的服務量，否則若於用量較大時發生故障狀況，剩餘的設備因負載過重無法正常提供服務，就失去備援的效果。
- Active-Passive 的備援架構也很常見，此方式是準備額外的代理設備，於線上主要設備無法服務時立刻取而代之。
- N+1或N+M的備援方式，則是以更大範圍的服務群組來考量，其備用設備需要額外多準備一至多組，不一定與服務主機數量是倍數關係。

確認可用性達成程度的安全指標(4/4)

- 透過監控與定期量測，完整即時的監控機制可以在部分設備或軟體元件出問題之初就發出警示
- 除了追求更短的服務中斷時間外，也應量測服務回應的速度，若因軟硬體或網路等因素造成服務回應過慢，也應納入**可用性受損的範圍**加以改善

- 可用性是很容易透過監控與定期量測而確認達成程度的安全指標，完整、即時的監控機制，往往可以在部分設備或軟體元件出問題之初就發出警示，讓系統管理人員儘快處理，這是維護可用性最表面、最末端，但也是最基本的機制。除了追求更短的服務中斷時間外，也應量測服務回應的速度，若因軟硬體或網路等因素造成服務回應過慢，也應納入可用性受損的範圍加以改善。

郵件完整性(1/3)

- 資訊安全的完整性 (Integrity) 指**資料應在其生命週期內(從資料產生、被利用及保存的期間)保持其正確與完整**，也就是防止被竄改、破壞及丟失，不論是內外部人員、因蓄意或意外所致
- 由於電子郵件已是現代主要的溝通工具，許多狀況下等同具法律效用的正式文件，因此也是重要的知識資產，必須持續妥善保護

- 資訊安全的完整性 (Integrity)，意指資料應在其生命週期內 (從資料產生、被利用及保存的期間)保持其正確與完整，也就是防止被竄改、破壞及丟失，不論是內外部人員、因蓄意或意外所致。由於電子郵件已是現代主要的溝通工具，許多狀況下等同具法律效用的正式文件，因此也是重要的知識資產，必須持續妥善保護。

郵件安全「完整性」的涵義(2/3)

- 郵件安全之「完整性」多數是指已傳遞到己方郵件主機、己方寄出之各項電子郵件相關資料之**保全與保存**
- **電子郵件相關資料**，除電子郵件本身，還包括：郵件收發紀錄、系統過濾或處置紀錄、郵件經過人工稽核之紀錄、郵件系統管理工作紀錄，以及各項資料或記錄經授權檢視之紀錄等

- 電子郵件資料之生命週期，分為收到及寄出的信件兩種狀況，收到的信件是由寄件人撰寫後，透過寄件方及郵件方郵件主機傳遞至收件人，由於傳遞過程十分快速且自動化，當中郵件遭他人攔截竄改後再遞送的案例很少見。比較常見的是過程中的寄件方或收件方郵件閘道可能會加註聲明，將違反政策或可能有危險內容的信件的郵件攔阻、留置或改為較不具威脅的內容。所以郵件安全之「完整性」多數是指已傳遞到己方郵件主機、己方寄出之各項電子郵件相關資料之保全與保存。此處所說電子郵件相關資料，除了電子郵件本身外，還包括：郵件收發紀錄、系統過濾或處置紀錄、郵件經過人工稽核之紀錄、郵件系統管理工作紀錄，以及各項資料或記錄經授權檢視之紀錄等。

危害郵件服務資料完整性的狀況(3/3)

- 來自於內外部人員可能為了不正當的目的，**蓄意竄改或破壞 (刪除)** 保存的電子郵件相關資料
- 因人員失誤或設備意外狀況，導致郵件資料丟失或變得不完整
- 為處理郵件資料的備份與保存、防止操作失誤、誤刪問題，可以由完整的郵件的備份機制解決

- 一般會危害郵件服務相關資料完整性的狀況，可能包括：來自於內外部人員可能為了不正當的目的，蓄意竄改或破壞 (刪除) 保存的電子郵件相關資料、因人員失誤或設備意外狀況，導致郵件資料丟失或變得不完整。為處理郵件資料的備份與保存、防止誤操作、誤刪問題，可以由完整的郵件的備份機制解決。

雲端應用(1/7)

- 綠能與環保
- 彈性付費
- 改善郵件服務穩定度
- 提高**郵件備援等級**
- 建立更具彈性的資訊團隊
- 加速郵件問題釐清與處理
- 越來越多國內機關正評估或甚至已導入郵件雲端服務

- 實際應用上改善郵件服務穩定度、提高郵件備援等級、建立更彈性的資訊團隊、並加速郵件問題釐清與處理，越來越多國內機關正評估或甚至已導入郵件雲端服務。

雲端電子郵件(2/7) (EaaS, Email as a Service)

- 經濟部工業局依據行政院國家資訊通信發展推動小組(NICI)於104年之指示，開始辦理軟體共同供應契約之雲端服務採購各項目，納入**雲端電子郵件 (EaaS, Email as a Service)** 為供應項目之一。
- 使用共同供應契約之方式簡化各機關採購程序，主辦單位於投標審核階段，要求各品項需通過專業、完整的各項檢測包括：雲端運算符合度測試、及資訊安全各項測試
- 維運廠商與所使用雲端機房，也需通過 ISO27001 國際資訊安全標準之驗證；藉此確保所有機關使用的雲端服務都具安全保障

- 經濟部工業局依據行政院國家資訊通信發展推動小組(NICI)於104年之指示，開始辦理軟體共同供應契約之雲端服務採購各項目之初，即納入雲端電子郵件 (EaaS, Email as a Service) 為供應項目之一。
- 使用共同供應契約之方式，不僅簡化各機關採購程序，主辦單位更於投標審核階段，要求各品項需通過專業、完整的各項檢測包括：雲端運算符合度測試、及資訊安全各項測試，包括弱點掃描(Vulnerability Assessment)、以及規格檢驗等，維運廠商與所使用雲端機房，也需通過 ISO27001 國際資訊安全標準之驗證；藉此確保所有機關使用的雲端服務都具安全保障。

雲端郵件服務之資安檢測(3/7)

- 為確保雲端服務品質，EaaS服務供應商需通過多項檢測
- 雲端服務**共通特性檢測**
- 雲端服務安全性檢測
- 滿足公務機關使用需求之雲端電子郵件(EaaS)雲端服務功能檢測

- 為確保雲端服務品質，EaaS服務供應商需通過多項檢測，主要包含雲端服務共通特性檢測、雲端服務安全性檢測及滿足公務機關使用需求之雲端電子郵件(EaaS)雲端服務功能檢測。

雲端服務安全性檢測指標(4/7)

編號	檢測指標	指標說明
1	資訊安全相關認證	提供雲端服務之所在地機房 ISO 27001 資安規範證照
2	安全通訊協定	雲端服務均須具備「傳輸層安全通訊協定(Transport Layer Security-TLS)」的安全通訊協定 v1.1 以上
3	系統及應用程式弱點	OWASP TOP10 2013 應用程式弱點掃描
		系統弱點掃描
4	防毒機制	廠商所提供之防毒產品，需包含於 3 大防毒軟體評鑑機構(AV-Comparatives、AV-TEST 與 Virus Bulletin)所公布最新檢測清單之非大陸廠商，且病毒碼為最新

- 機關要導入雲端郵件服務之前建議先評估，以確保郵件服務的移轉過程中是順暢的。

雲端服務與自建郵件系統差異(5/7)

- 資訊安全
- Anti-Spam
- 系統備援
- 郵件備份
- 人力費用
- 升級與維運

- 常見的雲端服務與自建郵件系統差異為，導入雲端服務的單位可將硬體維運、服務不中斷及專業客戶服務委託給雲端服務廠商，而選擇自行建置的機關則可以依據預算、需求及效益等考量彈性配置相關措施。

導入雲端服務前評估的要點(6/7)

- 機關環境之準備
- 系統轉移過程
- 使用者之準備
- 使用效益評估

電子郵件安全換證課程 103

- 機關要導入雲端郵件服務之前建議先評估以下要點，以確保郵件服務的移轉過程中是順暢的。
  - ✓ 機關環境之準備 。
  - ✓ 系統轉移過程。
  - ✓ 使用者之準備。
  - ✓ 使用效益評估。

導入雲端服務的資安與成本(7/7)

- 成本與管理人力的節省是雲端電子郵件系統很大的誘因
- 雲端服務都需要考量資料在地化的法規要求，以及資安管理分工分責的情況，必須審慎考量
- 雲端服務的業者變更，進行系統移置(migration)時需考量相關的影響因素

- 資安與成本的反思：一般機構建置電子郵件系統除了要為系統的效能與儲存需求安排適當的軟硬體環境之外，通常還要付出依帳號數目計價的使用授權費用。雲端電子郵件系統免除了這些成本的付出與相關的管理負荷，但是一旦郵件系統移往雲端，機構對系統就失去了部分的掌握，而且無法完全確認資料儲存的地點，若是機構電子郵件需要傳送個資或是機敏資料，勢必形成資安的威脅與風險。

行動裝置(1/9)

- 隨著智慧型手機以及平板電腦等行動裝置急速普遍，**電子郵件也跨入行動應用領域**
- 即使不在辦公室，也能收發郵件，即時處理重要事務
- 各機關該如何評估是否開放人員使用自己的行動裝置收發電子郵件，又應如何**規範與管理**

- 近年來隨著智慧型手機以及平板電腦等行動裝置急速普遍，電子郵件也跨入行動應用領域，即使不在辦公室，也能收發郵件，即時處理重要事務。各機關該如何評估是否開放人員使用自己的行動裝置收發電子郵件，又應如何規範與管理，可參照103年政府行動化安全防護規劃報告。

電子郵件相關行動資安應用要點(2/9)

- 先了解行動郵件功能與可行的管理方式
- 行事曆之應用
- 即時通訊 (Instant Messaging)
- 現行的行動裝置安全機制
- 制定**BYOD (Bring Your Own Device)** 及**行動裝置使用政策**

以行動裝置收發電子郵件(3/9)

- 透過專為行動裝置設計的行動裝置版Webmail
- 應用手機出廠時即內建的郵件軟體
- 另外安裝專門的手機應用程式 (App)

- 目前主要的郵件系統或雲端郵件服務，皆支援以行動裝置收發電子郵件。一般而言可分為3種方式使用：透過專為行動裝置設計的行動裝置版Webmail、應用手機出廠時即內建的郵件軟體或另外安裝專門的手機應用程式 (App) 。
- 使用行動裝置收發郵件，具有隨時、隨處的特性，除了增進溝通效率之外，也可以提升人員生產力；但機制愈方便，愈易使人忽略相關的安全風險。

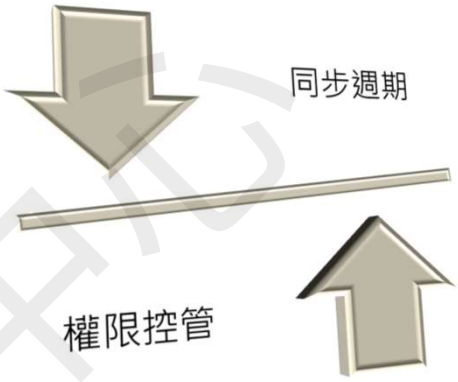
行動裝置對應的資訊安全功能(4/9)

- 可否僅開放部分使用者使用行動裝置收發信
- 行動裝置**收發信之軌跡紀錄**是否會完整保存於主機之系統中備查

- 管理人員應在推廣以行動裝置使用電子郵件之前，應先仔細了解郵件系統或雲端郵件服務在行動裝置方面對應的資訊安全功能，例如：可否僅開放部分使用者使用行動裝置收發信、行動裝置收發信之軌跡紀錄是否會完整保存於主機之系統中備查。

行事曆之應用(5/9)

- 使用者應注意行事曆的**同步週期**，避免資訊落差
- 並應確認分享行事曆時的**權限控管**，避免重要資訊無意間曝光



- 在手機或網頁介面都要有友善的使用環境，才能在彈指間完成操作，達成使用效率。使用者應注意行事曆的同步週期，避免資訊落差，並應確認分享行事曆時的權限控管，避免重要資訊無意間曝光。

即時通訊 (Instant Messaging)(6/9)

- 多數政府機關或民間企業皆樂見即時通訊可提升人員之溝通效率進而增加生產力
- 由於常見的即時通訊多半是**公有雲 (Public Cloud)**，是否能提供完整的資訊安全與管理機制、是否能符合政府機關所需的稽核與歸檔需求，皆是導入前需評估的要點
- 相較於為機關與企業組織設計的資訊應用，設計供個人使用的資訊服務如即時通訊，通常較易缺少以下幾個層面的資安功能

- 多數政府機關或民間企業皆樂見即時通訊可提升人員之溝通效率進而增加生產力，但由於常見的即時通訊多半是公有雲 (Public Cloud)，是否能提供完整的資訊安全與管理機制、是否能符合政府機關所需的稽核與歸檔需求，皆是導入前需評估的要點。相較於為機關與企業組織設計的資訊應用，設計供個人使用的資訊服務如即時通訊，通常較易缺少以下幾個層面的資安功能。

考量導入專為機關需求設計的即時通訊平台(7/9)

- 通訊過程是否留下紀錄日後可供對話各方或機關查證
- 通訊過程的機密性如何實作與如何管制
- 功能設計是否符合公務溝通及知識管理所需

- 機關在導入前可深入了解評估，考量導入專為機關需求設計的即時通訊平台。

現行的行動裝置安全機制(8/9)

- 確保只有授權人員能存取行動裝置
- 應用行動裝置管理**(Mobile Device Management, MDM)**系統
- 失竊與遺失時之緊急處置

- 由於行動裝置小巧、易於攜帶的特性，如果允許人員使用行動裝置辦理公務例如收發電子郵件或使用行動通訊，必須確保此行動裝置不會被未經授權的人員存取、裝置失竊或遺失時不致造成重大損害。

制定行動裝置使用政策(9/9)

- 機關充份收集資訊並評估後，可制定**行動裝置使用公務信箱**，以及BYOD相關的管理政策，讓相關管理人員及所有使用者有所依循
- 政策可設計為原則上鼓勵使用於工作用途，但需要先經過申請與核准的程序，並必須先確保手機至少具有密碼鎖定，指紋或虹膜等生物辨識功能更佳
- 若手機需使用於公務，必須保持作業系統的遠端抹除功能開啟，若該裝置失竊或遺失，至少可確保相關資料能在第一時間清除

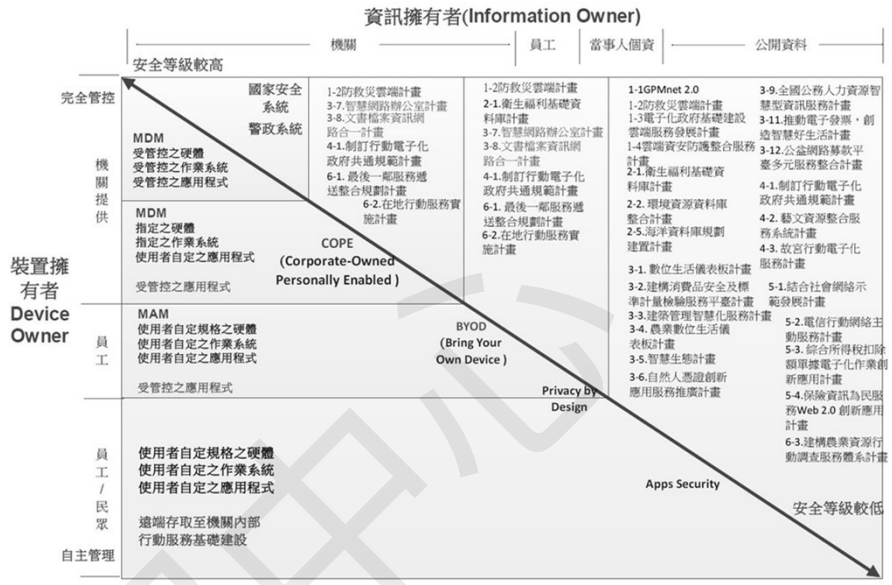
- BYOD是指Bring Your Own Device
- 機關充份收集資訊並評估後，可制定行動裝置使用公務信箱，以及BYOD相關的管理政策，讓相關管理人員及所有使用者有所依循。一般而言，管理政策應指示明確的方向，例如：鼓勵使用但應遵守特定程序或前提、原則允許但例外禁止或原則禁止但例外允許等。就現行民間企業常見做法而言，BYOD常被視為是提升生產力的作法，因此政策可設計為：原則上鼓勵使用於工作用途，但需要先經過申請與核准的程序，並必須先確保手機至少具有密碼鎖定，指紋或虹膜等生物辨識功能更佳。同時若手機需使用於公務，必須保持作業系統的遠端抹除功能開啟，若該裝置失竊或遺失，至少可確保相關資料能在第一時間清除。

BYOD、CYOD與COPE

- CYOD指choose your own device，讓使用者在企業選定的設備中選擇自己要使用的辦公設備
- COPE指Corporally owned, personally enabled
- COPE有企業將設備發給員工，並規定私人設備不可連入公司網路

- 不管是BYOD、CYOD還是COPE，以電子郵件系統來說，會有不同的資安考量與效果。

行政院行動裝置資安防護政策



電子郵件安全換證課程 115

- 行動應用情境分析是一種可以掌握機關現在以及可預見未來行動需求分析的方法，可以分別從資訊擁有者及裝置擁有者分析機關有哪些業務活動，可以採用行動化應用服務，以及需要採取的管理模式。

法規遵循相關項目

- 美國政府於2002年發布的沙賓法案(Sarbanes-Oxley Act of 2002, SOX)，提及組織須有政策規範保存Email並提供審查與稽核流程，同時包括美國金融服務法、HIPPA、NASD、FISMA等法規，也都提及Email的保存與保護
- 以**新巴賽爾協定(Basel II)**與**SOX沙賓法案**的要求，商務重要資料需保留5年、會計財務資料需保留7年，醫院、健保機構等也有類似的保存規定
- 政府機關宜參閱**「資訊系統風險評鑑參考指引」**與**「資通安全責任等級分級辦法」**之方法，對於電子郵件系統之安全等級進行評定，並採取適當的措施

- 美國政府於2002年發布的沙賓法案(Sarbanes-Oxley Act of 2002, SOX)、及隨後日本政府的日本版沙賓法案中，皆提及組織須有政策規範保存Email並提供審查與稽核流程，同時包括美國金融服務法、HIPPA、NASD、FISMA等法規，也都提及Email的保存與保護。以新巴賽爾協定(Basel II)與SOX沙賓法案的要求而言，商務重要資料需保留5年、會計財務資料則需保留7年，在醫療體系如醫院、健保機構等單位中，也有類似的保存規定。
- 政府機關宜參閱「資訊系統風險評鑑參考指引」與「資通安全責任等級分級辦法」之方法，對於電子郵件系統之安全等級進行評定，並採取適當的措施。

透過共同供應契約的資安服務採購

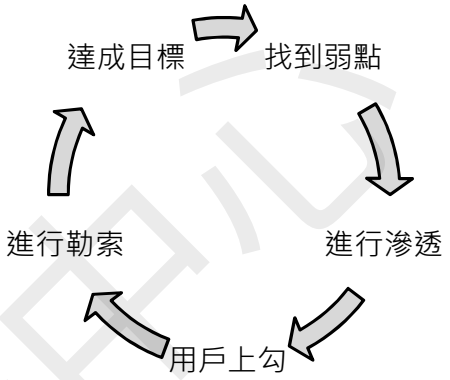
- 目的:提供政府機關以迅速便捷方式採購資安服務
- 方式: 政府機關自行至政府電子採購網勾選所需服務
- **資安服務品項**
  - 資安健診服務
  - 資安監控服務
  - 弱點掃描服務
  - 滲透測試服務
  - 社交工程郵件測試服務

電子郵件安全換證課程 117

- 透過共同供應契約的資安服務採購可以比較快速地透過政府對採購項目的評估，在比較沒有安全疑慮的情況下完成資安服務採購。

勒索軟體透過電子郵件系統攻擊

- 勒索軟體可以運用APT(advanced persistent threat)搭配電子郵件進行攻擊
- 電子郵件系統必須防範勒索軟體的攻擊



電子郵件與數位證據保存

- 數位證據(digital evidence)所指的是由電腦來儲存或是傳送的**資料**
  - 該資料可以用來進行後續的偵查
  - 偵查的目的是用來確認或是否定反駁有關於犯罪的推斷陳述
  - **該資料在法庭上有具體的用途**
- 電子郵件與附件也是資料的一種類型，可能成為數位證據